RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

1•2025

SEZIONI MONOGRAFICHE

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II

edited by Elda Brogi

❑

Digitalizzazione del processo e diritti fondamentali – Profili sostanziali

a cura di
Francesca Bailo e Michele Francaviglia

diretta da **Sebastiano Faro • Marina Pietrangelo**

direzione e redazione
Istituto di Informatica Giuridica e Sistemi Giudiziari
Via dei Barucci 20 • 50127 Firenze

anno VII • periodicità semestrale • ISSN 2704-7318

www.rivistaitalianadiinformaticaediritto.it

Consiglio Nazionale delle Ricerche

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

Organi

DIREZIONE

Sebastiano Faro IGSG-CNR
Marina Pietrangelo IGSG-CNR

Comitato di direzione

Federigo Bambi Università di Firenze
Elda Brogi European University Institute
Simone Calzolaio Università di Macerata
Enrico Carloni Università di Perugia
Davide Carnevali IGSG-CNR
Gian Luca Conti Università di Pisa
Enrico Francesconi IGSG-CNR
Antonio Iannuzzi Università Roma-Tre
Erik Longo Università di Firenze
Lorenzo Nannipieri IGSG-CNR
Stefano Pietropaoli Università di Firenze
Francesco Romano IGSG-CNR

Comitato scientifico

Laura Abba IGSG-CNR
Agata C. Amato Mangiameli Università di Roma-Tor Vergata
Fabio Bravo Università di Bologna
Andrea Cardone Università di Firenze
Antonio Carcaterra UnitelmaSapienza
Paolo Caretti già Università di Firenze
Massimo Carli già Università di Firenze
Elisabetta Catelani Università di Pisa
Adriana Ciancio Università di Catania
Renato Clarizia Università Roma-Tre
Carlo Colapietro Università Roma-Tre
Giovanni Comandé Scuola Superiore Sant'Anna
Giuseppe Corasaniti UnitelmaSapienza
Pasquale Costanzo già Università di Genova
Giovanna De Minico Università di Napoli - Federico II
Rosa Maria Di Giorgi già IGSG-CNR
Elio Fameli già IGSG-CNR
Carla Faralli Università di Bologna
Giusella Finocchiaro Università di Bologna
Tommaso E. Frosini Università di Napoli-Suor Orsola Benincasa
Mario Jori già Università di Milano
Donato A. Limone UnitelmaSapienza
Aldo Loiodice Università Europea Roma
Luigi Lombardi Vallauri già Università di Firenze
Nicola Lupo Università di Roma-LUISS
Nicoletta Maraschio Accademia della Crusca
Paola Marsocci Università Roma-Sapienza
Gaetana Morgante Scuola Superiore Sant'Anna
Paolo Moro Università di Padova
Monica Palmirani Università di Bologna
Ugo Pagallo Università di Torino
Giovanni Pascuzzi Consiglio di Stato
Paolo Passaglia Università di Pisa
Oreste Pollicino Università di Milano-Bocconi
Benedetto Ponti Università di Perugia
Giovanni Sartor Università di Bologna
Andrea Simoncini Università di Firenze
Carlo Sorrentino Università di Firenze
Giancarlo Taddei Elmi già IGSG-CNR
Lara Trucco Università di Genova
Stefano Trumpy Internet Society Italia
Alessandra Valastro Università di Perugia
Franco Vallocchia Università Roma-Sapienza
Giovanni Ziccardi Università di Milano

Esperti per la valutazione

L'elenco degli esperti è reperibile sul sito della Rivista

Con la pubblicazione della nuova *Rivista italiana di informatica e diritto*, l'IGSG-CNR prosegue l'attività editoriale avviata nel 1972 con la pubblicazione prima del *Bollettino bibliografico d'informatica generale e applicata al diritto* e poi, dal 1975, della rivista *Informatica e diritto* nata come organo dell'allora Istituto per la Documentazione Giuridica (IDG-CNR), poi diventato Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG-CNR), confluito ora nell'IGSG-CNR.

Al momento della sua nascita, nel 1975, l'aspirazione dei promotori della rivista *Informatica e diritto* era di «iniziare in Italia un discorso critico, scientificamente fondato, sull'informatica e sui rapporti di questa nuova disciplina e realtà sociale col diritto» con la convinzione di «colmare il vuoto culturale esistente nel panorama delle riviste italiane e, in particolare, di quelle giuridiche» (così si legge nella presentazione firmata dal comitato direttivo formato da Luigi Lombardi Vallauri, Mario G. Losano e Costantino Ciampi). La Rivista mirava a rispondere alla «esigenza di un approccio all'informatica da parte del giurista che fosse unitario e non più separato per sfere di interesse», secondo un modello che andava emergendo in altri Paesi, continuando l'esperienza già avviata nel 1972 con il *Bollettino bibliografico d'informatica generale e applicata al diritto*.

Nell'arco di oltre quarant'anni *Informatica e diritto* ha ampiamente realizzato le funzioni che per essa intravedevano i suoi promotori. Con funzione informativa, essa ha fatto conoscere ai lettori idee, problemi e fatti del mondo dell'informatica giuridica e del diritto dell'informatica, dando conto anche dello sviluppo delle ricerche in un settore allora emergente e delle prospettive – non solo giuridiche, ma anche politiche e sociali – a esso collegate. Con la non meno importante funzione di approfondimento scientifico, promozione e coagulo di ricerche specialistiche e settoriali la Rivista ha dato spazio a idee e riflessioni che hanno avuto un ruolo significativo nella evoluzione dell'informatica giuridica in Italia e all'estero. Alcuni saggi pubblicati in *Informatica e diritto* sono ancora oggi autentiche pietre miliari nella storia dell'informatica giuridica e del diritto dell'informatica, a testimonianza dell'importanza e dell'impatto che essa ha avuto nel dibattito scientifico sui temi del rapporto fra diritto e tecnologie dell'informazione e della comunicazione.

Nell'arco di oltre quarant'anni *Informatica e diritto* ha ampiamente realizzato le funzioni che per essa intravedevano i suoi promotori. Con funzione informativa, essa ha fatto conoscere ai lettori idee, problemi e fatti del mondo dell'informatica giuridica e del diritto dell'informatica, dando conto anche dello sviluppo delle ricerche in un settore allora emergente e delle prospettive – non solo giuridiche, ma anche politiche e sociali – a esso collegate. Con la non meno importante funzione di approfondimento scientifico, promozione e coagulo di ricerche specialistiche e settoriali la Rivista ha dato spazio a idee e riflessioni che hanno avuto un ruolo significativo nella evoluzione dell'informatica giuridica in Italia e all'estero. Alcuni saggi pubblicati in Informatica e diritto sono ancora oggi autentiche pietre miliari nella storia dell'informatica giuridica e del diritto dell'informatica, a testimonianza dell'importanza e dell'impatto che essa ha avuto nel dibattito scientifico sui temi del rapporto fra diritto e tecnologie dell'informazione e della comunicazione. Nel corso della sua storia la Rivista è stata accompagnata da un prestigioso gruppo di corrispondenti stranieri: Y. Amoroso, T.J.M. Bench Capon, D. Bourcier, W.E. Boyd, V. De Mulder, J. Dumortier, F. Galindo, A. Gardner, T. Gordon, G. Greenleaf, O.P. Hance, W. Kilian, F. Lachmayer, P. Leith, E. Mackaay, A. Maclntosh, P. Maharg, J. Mayor, L.T. McCarty, F. Novak, A. Paliwala, A.E. Perez-Luño, R. Petrauskas, L. Philipps, Y. Poullet, A. Saarempaa, E. Schweighofer, P. Seipel, R. Susskind, W.R. Svoboda, H. Yoshino, T. Van Engers, M.A. Wimmer, R. Winkels, J. Zeleznikow.

Nel 2019, l'Istituto di Informatica Giuridica e Sistemi Giudiziari (IGSG) ha aperto una nuova pagina nella storia della sua rivista, affidata adesso alla Rete nell'ottica di una politica di accesso aperto alle pubblicazioni scientifiche (secondo il modello del "Diamond Open Access"): è nata, quindi, la *Rivista italiana di informatica e diritto* che rappresenta il diretto proseguimento di *Informatica e diritto* da cui eredita il programma scientifico, l'approccio e l'ampia apertura alla realtà internazionale, oltre che i componenti degli organi scientifici, arricchiti di nuove personalità scientifiche rispetto alla formazione originaria.

Segreteria di redazione Simona Binazzi e Mariasole Rinaldi
Elaborazione testi e grafica Teresa Balsamo e Giuseppina Sabato
Responsabile del sito web Elisabetta Marinai
Direzione e Redazione IGSG/CNR • Via dei Barucci, 20 • 50127 Firenze • Tel. +39 055 43995
rivistaRIID@igsg.cnr.it • www.rivistaitalianadiinformaticaediritto.it
Direttore responsabile Sebastiano Faro • Registrazione presso il Tribunale di Roma al n. 127/2019

1•2025

Indice

Sezioni monografiche

Digitalizzazione del processo e diritti fondamentali - Profili sostanziali

a cura di Francesca Bailo e Michele Francaviglia

Digitalizzazione del processo e diritti fondamentali - Profili sostanziali. Introduzione [Francesca Bailo] 9
IA e funzioni giurisdizionali: alcune questioni preliminari alla luce del quadro costituzionale [Michele Francaviglia] 13
Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni? [Omar Caramaschi] 29
Brevi osservazioni sulla c.d. "confessione intercettata": un dibattito ancora attuale tra spontaneità e consapevolezza [Alessandro Malacarne] 53

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? - Part II

a cura di Elda Brogi

Market power and opinion power. Assessing the risks for media pluralism and editorial independence deriving from ownership's concentration [Roberta Carlini] 75
Il principio del pluralismo rovesciato. Alla riscoperta dell'ordinamento costituzionale della politicità [Simone Calzolaio] 87
Grounding media freedom in the EU: The legal basis of the EMFA [Erik Longo] 111
What is journalism in the digital age? Key definitions in the European Media Freedom Act [Sofia Verza] 125
New and reinforced rights for media service providers under Article 4 European Media Freedom Act [Luigi Malferrari] 143
The delicate balancing between media pluralism and market freedom: Analysing the procedural safeguards for the media under Article 21 of the EMFA [Jan Erik Kermer] 177
The governance framework of the European Media Freedom Act [Matteo Trevisan] 195
Micro-targeting politico e protezione dei dati personali. Il Regolamento (UE) 2024/900 [Camilla Lobascio] 205

Studi e ricerche

Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa [Maria Chiara Pollicino] 231
Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative [Enza Cirone] 257

Possibili funzioni di un istituto internazionale per la sicurezza dell'intelligenza artificiale. Un'analisi istituzionale dell'AIEA e dell'IPCC nel contesto delle recenti tendenze sulla governance dell'intelligenza artificiale [Arcangelo Leone De Castris] 279

Decentralized Autonomous Organization, *blockchain* e impresa: considerazioni giuridico-economiche [Antonio Manganelli] 291

The future without a Judge [Fabrizio Corona, Moreno Ferrarese] 309

Oltre il consenso. I limiti dell'*Individual Control Model* e prospettive per un approccio collettivistico alla sorveglianza contemporanea [Leonardo Marchesin] 361

Bridging borders, streamlining justice, balancing interests. The e-Evidence package journey: from a troubled origin story to an uncertain future [Rosanna Amato] 385

Le prospettive di collaborazione tra Autorità indipendenti nell'era digitale [Marco Guerra] 411

Libertà di espressione e nuove tecnologie: *a complicated relationship* [Antonio Cremone] 441

Evaluating the performance of DeepL as translation tool between German and Italian Easy Language administrative texts [Christiane Maaß, Chiara Fioravanti] 475

Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza [Veronica Montozzi] 501

Il nuovo design europeo del mercato dell'energia elettrica e i contratti flessibili: il caso del progetto pilota di Areti "Romeflex" [Ercole De Luca, Luisa Lodevole] 525

La nuova Intelligenza artificiale e il problema della sua regolazione giuridica. La strategia europea e il lungo iter legislativo dell'AI Act [Elio Fameli] 551

È (ancora) tempo di costituzionalismo digitale [Chiara Spiniello] 579

Sistemi e applicazioni

Inteligencia artificial generativa aplicada a la valoración probatoria en un caso de prescripción adquisitiva [Dario Saul Navarro, José Osvaldo Ledesma] 601

Note e discussioni

Blockchain e buona fede: riuscirà la tecnologia a sostituire la fiducia? [Massimiliano Marletta] 615

Regolamento generale sulla protezione dei dati e cybersecurity nelle pubbliche amministrazioni: le nuove sfide, le opportunità e best practices delle istituzioni scolastiche, nel contesto delle risorse del PNRR [Paola D'Abbrunzo] 627

I processi decisionali automatizzati nel GDPR, spunti e riflessioni interpretative [Alessandro Manfredi] 637

Cenni sulla funzionalità dell'atto amministrativo con l'ausilio dei Sistemi Esperti [Alfonso Contaldo] 657

Sezione monografica

Digitalizzazione del processo e diritti fondamentali. Profili sostanziali

a cura di

Francesca Bailo e Michele Francaviglia

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0230 • articolo non sottoposto a peer review • pubblicato in anteprima il 30 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Francesca Bailo

Digitalizzazione del processo e diritti fondamentali
Profili sostanziali
Introduzione

L'Autrice è professoressa associata di Diritto costituzionale presso il Dipartimento di Giurisprudenza – Università degli studi di Genova

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili sostanziali* a cura di Francesca Bailo e Michele Francaviglia

Questa seconda sezione monografica fa seguito a una prima e corposa sezione dedicata agli atti, debitamente aggiornati e rielaborati, del Seminario "*Process digitalization and fundamental rights*" tenutosi presso l'Università di Genova il 9 maggio 2024 e organizzato nell'ambito del progetto "*Law and regulation for a better-safe Cyberspace*" (CYBERIGHTS - Partenariato esteso SERICS, Spoke 1) in sinergia con il progetto PRIN PNRR 2022 su "*Digitalization of the judiciary functions: trends, perspectives and risks*", pubblicata nel fascicolo 2/2024 di questa prestigiosa Rivista.

Essa perciò muove dagli esiti delle ricerche già svolte in quella sede (concentratesi, in particolare, sull'analisi degli aspetti processualistici legati alla digitalizzazione della giustizia e, ancor prima, alla disamina del rilievo costituzionale dell'accesso alla rete come risorsa indispensabile), per meglio ora mettere a fuoco, innanzitutto, le sfide poste dall'avvento dell'intelligenza artificiale in punto di regolamentazione, nel bilanciamento costituzionale tra l'interesse economico relativo allo sviluppo di un mercato digitale e quello di tutelare i valori democratici e i diritti e le libertà fondamentali degli individui (Caramaschi). Un approfondito vaglio sarà, inoltre, svolto sull'impatto che le nuove tecnologie determinano (o potrebbero determinare) sulle garanzie costituzionali più direttamente legate all'esercizio della funzione giurisdizionale (Francaviglia). In ultimo l'attenzione sarà portata sulla pervasività dei nuovi strumenti investigativi "tecnologici" in quanto capaci di coartare, anche solo indirettamente, la volontà del prevenuto, sì da mettere in discussione la garanzia stessa del fondamentale diritto al silenzio.

Un tale prezioso e corale contributo di esperti di vari settori del diritto consente così di fissare almeno due punti fondamentali rispetto al complesso – e tuttora *in fieri* – percorso di ammodernamento del "servizio giustizia".

Deve cioè tenersi conto, da un lato, del fatto che sul piano processualistico è a tutt'oggi stato mantenuto un "doppio binario" o, se si preferisce, una sorta di "ibridazione" tra cartaceo e digitale e, dall'altro, che la stessa ormai traguardata e pressoché integrale digitalizzazione di tutti i processi giurisdizionali può considerarsi come un mero *step* verso il più ambizioso obiettivo dell'impiego dell'intelligenza artificiale "a supporto" (e, si badi, giammai "in sostituzione") della macchina giudiziaria.

Quanto al primo versante, può, infatti, osservarsi che la stessa Corte costituzionale ne ha dimostrato una piena consapevolezza, tra le altre, nella sentenza n. 96 del 2022. Nel dichiarare l'inammissibilità della questione di legittimità costituzionale relativa all'art. 153 c.p.p., nella parte in cui ancora non consentiva alle parti o ai difensori di eseguire le notificazioni al pubblico ministero mediante posta elettronica certificata (PEC), dava, infatti, atto del mutato quadro normativo nel frattempo intervenuto per affrontare l'emergenza pandemica e ammoniva il legislatore delegato a confermare (come poi effettivamente avvenuto con l'art. 10, comma 1, del d.lgs. 10 ottobre 2022, n. 150) anche per il futuro la facoltà per il difensore di giovarsi di dette modalità telematiche "in coerenza con il dovere costituzionale di assicurare piena effettività al diritto di difesa, e assieme di superare definitivamente l'irragionevole disparità di trattamento tra parte pubblica e privata ravvisata, a ragione, dal giudice rimettente". Epperò che la digitalizzazione non debba costituire una barriera per coloro che avrebbero il diritto di adire l'autorità giurisdizionale senza il patrocinio del difensore è stata la stessa Corte di Strasburgo ad affermarlo, sottolineando come un formalismo eccessivo e/o comunque sproporzionato nell'uso della comunicazione elettronica potrebbe compromettere la stessa equità del processo oltreché l'accesso alla giustizio, senza al contempo dar almeno prova di garantire la certezza del diritto e la buona amministrazione della giustizia (Corte EDU, V sez., dec. 9 giugno 2022, n. 15567/20, *Xavier Lucas c. Francia*).

È noto poi come, al di là delle necessarie clausole codicistiche "di chiusura", il regime analogico sia stato spesso chiamato a "supplire" i malfunzionamenti e/o i disfunzionamenti "tecnici" del digitale, specie nel più recente processo penale telematico, tanto che taluni presidenti di tribunale si sono visti costretti addirittura a sospendere l'utilizzo dell'applicativo telematico. Numerose, inoltre, sono le pronunce di inammissibilità o irricevibilità pronunciate dalle autorità giurisdizionali per vizi riscontrati nell'impiego delle nuove tecnologie e per lo più riconducibili a carenze nella formazione del personale (principalmente avvocati e/o cancellieri e/o comunque soggetti "obbligati" ad avvalersi del digitale).

Ad ogni modo, e venendo al secondo versante, occorre segnalare come il forte impulso alla digitalizzazione della giurisdizione, comune per lo più a tutti gli altri ordinamenti (eurounitari e non) specie nella fase post-pandemica, sia andato di pari passo, sempre in una prospettiva comparata, con l'implementazione e la almeno parziale regolamentazione di sistemi di giustizia predittiva e/o comunque basati sull'intelligenza artificiale.

Significativa, in tal senso, è, esemplarmente, l'esperienza maturata oltralpe. Con la l. n. 2016-1321 del 7 ottobre 2016 (legge per una Repubblica digitale) è stata, infatti, imposta la trasparenza degli algoritmi pubblici, offrendosi così una garanzia contro un possibile fenomeno di "scatola nera" negli usi giudiziari dell'intelligenza artificiale, mentre con l'ordinanza n. 2018-1125 del 12 dicembre 2018 (di modifica dell'art. 47 della l. 78-17 del 6 gennaio 1978 relativa all'informatica, ai fascicoli e alle libertà), in modo ancor più rigoroso di quanto al proposito disposto nel GDPR, si è stabilito che nessuna decisione giudiziaria che comporti una valutazione del comportamento di una persona possa essere basata su un trattamento automatizzato di dati personali destinato a valutare determinati aspetti della personalità di tale persona e che, salvo le deroghe esplicitate, nessuna decisione che produca effetti giuridici che riguardino una persona o che incida in modo analogo significativamente sulla stessa possa essere presa basandosi unicamente sul trattamento automatizzato dei dati personali, compresa la profilazione. E, ancora, con la l. n. 2019-222 (di programmazione 2018-2022 e di riforma della giustizia) sono state previste sanzioni penali per coloro che, partendo dalle decisioni, raccolgano, analizzino e riutilizzino "i dati di identità dei magistrati con lo scopo o l'effetto di valutare, analizzare, confrontare o prevedere le loro pratiche effettive o presunte pratiche professionali".

Parimenti, un importante spunto di riflessione proviene dalla decisione del primo Senato del Tribunale costituzionale federale tedesco del 16 febbraio 2023, con cui è stata dichiarata l'illegittimità costituzionale di disposizioni contenute nelle leggi di pubblica sicurezza dei Länder Assia e Amburgo, nella parte in cui consentivano l'analisi automatizzata di dati personali ai fini della prevenzione di reati; mentre si è giudicato legittimo il ricorso all'analisi automatizzata dei dati archiviati ove questa sia limitata allo scopo di prevenire determinati reati e il legislatore abbia definito in modo sufficientemente preciso i presupposti che giustifichino tale misura fortemente limitativa dei diritti fondamentali, secondo uno scrutinio di proporzionalità "in senso stretto".

Tra gli ordinamenti di *common law*, particolarmente dirimente è, inoltre, l'esperienza maturata nel Regno Unito, in ordine, in particolare, al *predictive coding*, su cui è stata chiamata a pronunciarsi l'Alta Corte nel noto caso *Pyrrho Investments Limited v MWB Property Limited*, ma anche per il fatto che è stata pubblicata una guida per i magistrati sull'utilizzo dell'intelligenza artificiale (*Guidance for Judicial Office Holders on Use of Artificial Intelligence*).

In un tale affastellato quadro regolatorio, sembra collocarsi su una soluzione piuttosto compromissoria il legislatore nazionale, dal momento che, con il precipuo intento di dare attuazione/integrazione all'AI Act, sta portando avanti i lavori alla proposta di legge A.S. 1146 (al momento in cui si scrive approvata in prima lettura dal Senato il 20 marzo 2025 e riapprovata, con modificazioni, dalla Camera il 25 giugno 2025 (A.C. 2316)). Di particolare interesse è l'art. 15 dell'articolato, integralmente riscritto nell'esame al Senato, il quale si propone di stabilire che, in caso di utilizzo dei sistemi di intelligenza artificiale, siano sempre riservate al magistrato le decisioni concernenti l'interpretazione e l'applicazione della legge; la valutazione dei fatti e delle prove; l'adozione dei provvedimenti, sì da escludersi in qualsiasi misura, se non si va errando, il ricorso a forme di giustizia predittiva. È invece espressamente consentito il ricorso a sistemi di intelligenza artificiale per ciò che riguarda, in particolare, l'organizzazione dei servizi relativi

alla giustizia; la semplificazione del lavoro giudiziario e le attività amministrative accessorie, oltreché (fino alla compiuta attuazione del regolamento europeo sull'intelligenza artificiale) l'autorizzazione alla sperimentazione e l'impiego dei sistemi di intelligenza artificiale negli uffici giudiziari ordinari in capo al Ministero della giustizia. Si tratterebbe, dunque, di un approccio pur sempre antropocentrico alle nuove tecnologie che, specie rispetto alle esperienze ordinamentali più sopra richiamate e rispetto allo stesso AI Act, parrebbe più rigoroso e restrittivo ma che forse lascerebbe talune "zone grigie", consentendo un allargamento delle maglie delle deroghe in cui parrebbe circoscritto il legittimo ricorso a detti sistemi, rimanendo pur sempre in linea, almeno nei profili più generali, con il quadro costituzionale ed euronitario in cui lo stesso si andrebbe ad inscrivere.

Nei contributi che seguono sono pienamente tratteggiati i capisaldi di dette garanzie che, in ogni caso, dovrebbero rappresentare un "faro" per il buon esito di una tale (co)regolamentazione, con l'avvertenza che il maggior rischio per ogni norma è proprio quella di conservare quella "attualità" che spesso risulta particolarmente scivolosa quando si deve "rincorrere" strumenti che nel momento in cui vengono apparentemente imbrigliati dal legislatore paiono rapidamente cadere nell'obsolescenza perché superati da sistemi sempre più avanguardisti.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0225 • articolo sottoposto a peer review • pubblicato in anteprima l'11 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Michele Francaviglia

IA e funzioni giurisdizionali: alcune questioni preliminari alla luce del quadro costituzionale

Il contributo esamina le questioni costituzionali preliminari relative alla delega di funzioni giurisdizionali all'intelligenza artificiale (IA), analizzandone in particolare il potenziale impatto sui principî cardine del potere giudiziario italiano. In particolare, si argomenta che il principio di esclusiva soggezione del giudice alla legge (art. 101 Cost.) implichi un rapporto di vicendevole implicazione tra giudice-persona e legge, difficilmente sostituibile dalla macchina, anche per la capacità della seconda di elaborare dubbi. In questo senso, la Costituzione evidenzia una concezione rigorosamente antropomorfa delle funzioni giurisdizionali. L'analisi si concentra, poi, sulla tensione tra la "calcolabilità" del diritto tramite IA e la natura interpretativa ed evolutiva dell'attività giudiziaria, cruciale per gli assetti interpretativi riguardanti i diritti fondamentali. La delega integrale all'IA potrebbe compromettere queste dinamiche e la comprensibilità delle motivazioni. Pur riconoscendo l'utilità dell'IA quale ausilio del giudice in fasi specifiche del processo, l'articolo sottolinea la centralità dell'elemento umano nell'esercizio della giurisdizione, così come la necessità di interventi legislativi che affrontino olisticamente il tema dell'IA nell'ambito delle funzioni giudiziarie.

Costituzione – Processo – Intelligenza artificiale – Interpretazione – Diritti fondamentali

AI and judicial functions: some preliminary issues in light of the constitutional framework

The paper examines the preliminary constitutional questions concerning the delegation of judicial functions to artificial intelligence (AI), particularly analyzing its potential impact on the core principles of the Italian judiciary. Specifically, it is argued that the principle of the judge's exclusive subjection to the law (Article 101 of the Constitution) implies a relationship of mutual implication between the judge-human being and the law, difficult to replace by machines, also due to the latter's capacity to elaborate doubts. In this sense, the Constitution highlights a strictly anthropomorphic conception of judicial functions. The analysis then focuses on the tension between the "calculability" of law through AI and the interpretative and evolutionary nature of judicial activity, crucial for the interpretative frameworks concerning fundamental rights. The complete delegation to AI could compromise these dynamics and the comprehensibility of reasoning. While acknowledging the utility of AI as an aid to the judge in specific phases of the process, the article emphasizes the centrality of the human element in the exercise of jurisdiction, as well as the necessity of legislative interventions that holistically address the issue of AI within judicial functions.

Constitution – Trial – Artificial intelligence – Interpretation – Fundamental rights

L'Autore è professore associato di Diritto costituzionale e pubblico nell'Università degli studi di Genova

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili sostanziali* a cura di Francesca Bailo e Michele Francaviglia

Questo lavoro rappresenta la versione rivista, ampliata e aggiornata della relazione tenuta al seminario *Process digitalization and fundamental rights*, svoltosi presso l'Università degli studi di Genova il 9 maggio 2024, e costituisce attività di ricerca nell'ambito del Progetto PRIN PNRR 2022 Digitalization of the judiciary functions: trends, perspectives and risks (CUP: D53D23022420001; Codice progetto: P2022PRBCS)

Sommario: 1. Oggetto del contributo e finalità dell'indagine. – 2. Costituzione, principio antropomorfico e funzioni giurisdizionali. – 3 Intelligenza artificiale e il dibattito sull'interpretazione giuridica: nuove premesse e nuovi problemi. – 4. Intelligenza artificiale, interpretazione costituzionale e garanzia dei diritti fondamentali. – 5. Possibili impieghi dell'IA nell'ambito delle funzioni giurisdizionali: una questione di metodo. – 6. Alcune conclusioni alla luce del PNRR: sull'attualità della distinzione tra funzioni giurisdizionali e "servizi relativi alla giustizia".

1. Oggetto del contributo e finalità dell'indagine

La delega dell'esercizio di funzioni giurisdizionali a forme di intelligenza artificiale (IA) è una frontiera ancora lontana rispetto all'attuale grado di sviluppo degli ordinamenti giuridici occidentali, specie di quelli europei. Tuttavia, essa non è del tutto irraggiungibile: alcune esperienze nel mondo – come per es. il caso *Loomis*[1] o l'iniziativa del governo estone di utilizzare un algoritmo per risolvere controversie di valore economico ridotto[2] – dimostrano infatti che l'automatizzazione delle decisioni giurisdizionali (il cosiddetto giudice-automa) rappresenti già oggi una possibile evoluzione dei sistemi giuridici, inclusi quelli che garantiscono un'adeguata protezione al principio dello Stato di diritto.

Il tema, com'è ovvio, dischiude un'ampia gamma di questioni solo in parte di ordine giuridico-formale, estendendosi anche all'ambito tecnico-pratico ed etico-filosofico. Tali incertezze, peraltro, allignano anche con riferimento alle più basilari premesse definitorie circa il fenomeno dell'IA: l'evoluzione di siffatta tecnologia è talmente rapida da rendere facilmente obsolete, e comunque imprecise, le analisi portate avanti dalle scienze sociali. L'IA, come fenomeno tecnologico, non conosce ancora (e non lo conoscerà per molto tempo) un periodo di stabilizzazione, risultando così per definizione sfuggente, ancipite. Le difficoltà che tale situazione è in grado di determinare sui processi (normativi, giurisprudenziali e dottrinali) di formalizzazione del fenomeno sul piano giuridico sono dunque evidenti[3].

A tal riguardo, si pensi a titolo di esempio al concetto di intelligenza artificiale "predittiva", intesa come quella tecnologia in grado di "calcolare", su base statistico-probabilistica e attraverso la sua stessa capacità di autoapprendimento (*machine learning*), lo sviluppo o l'evoluzione di un dato fenomeno[4]. Applicare il concetto in questione (e la tecnologia ad esso sottesa) al fenomeno giuridico

1. Cfr. *State of Wisconsin c. Loomis*, 881 N.W.2d 749 (Wis. 2016); sul caso v. le considerazioni di Simoncini 2019, p. 78 ss.
2. Su questo caso cfr. Martino 2020, p. 15 ss.
3. Il tema delle possibili applicazioni (e implicazioni) dell'IA al fenomeno giuridico è indagato ormai da tempo e in modo ampio in dottrina; con riferimento al dibattito giuspubblicistico italiano cfr., senza alcuna pretesa di completezza; Fabrizzi–Durst 2024; Sterpa 2024; Cerri 2023, p. 39 ss.; Pollicino 2023, p. 410 ss.; Ladu–Maccabiani 2023; Martire 2022; D'Aloia 2022, p. 651 ss.; Simoncini 2020; Simoncini 2019, p. 63 ss.; Ruffolo 2021–a; Papa 2022; Grimaldi 2022, p. 75 ss.; Civitarese Matteucci 2019, p. 5 ss.; Carleo 2019; Costantino 2019, p. 43 ss.; con specifico riferimento alla prospettiva giurisdizionale, v. poi Luciani 2018, p. 871 ss.; Pajno 2022; Napoli 2020; Donati 2020.
4. Proprio su questa forma di IA v. da ultimo Durst 2024, p. 11 ss.

produce una serie di dilemmi di ordine semantico (e dunque, ai fini del giurista, sistemico) di non poco conto: se, infatti, con il termine "predittività", si fa riferimento alla predicibilità degli esiti applicativi di una determinata *forma di IA* a una domanda o un problema di tipo giuridico (*quid iuris*?), oggetto di studio da parte della scienza giuridica sarà la medesima IA e in particolare le modalità attraverso le quali essa persegue quel determinato scopo (risolvere un problema giuridico); se, invece, con il termine in questione, si fa riferimento alla predicibilità degli esiti applicativi di una determinata *norma giuridica* (o di un sistema di norme), l'IA diviene solo uno dei possibili strumenti attraverso cui conoscere il significato normativo di una data disposizione (rispetto a una determinata fattispecie concreta), sicché sarà quest'ultimo che resta l'oggetto principale dello studio del giurista.

Da questo punto di vista, l'utilizzo dell'IA (e in particolare di quella di tipo predittivo) nell'esercizio di funzioni giurisdizionali è un'ipotesi di studio peculiare poiché in essa emerge in modo chiaro il rischio che le due accezioni di "predittività" cui si è fatto cenno siano confuse all'interno di un unico piano di analisi.

Al contrario, si tratta di due concetti, non solo – sebbene per ragioni diverse – probabilmente irraggiungibili, ma anche radicalmente diversi: da un lato, determinati modelli complessi di *machine learning*, in particolare le reti neurali profonde, presentano dei meccanismi di funzionamento interno del tutto oscuri alla logica umana; dall'altro lato, come si ricorderà anche più avanti, l'idea tutta moderna di un diritto perfettamente "calcolabile" [5], inteso come esito applicativo razionalmente prevedibile di un determinato significante normativo, ha perso molta della sua forza negli ordinamenti giuridici contemporanei.

A ben vedere, dunque, nelle due accezioni di predittività cui si è accennato si riflettono altrettante forme di "oscurità"[6], il cui *trait d'union* (o la cui porta d'ingresso nell'esperienza giuridica) potrebbe essere rappresentato proprio da un utilizzo non sorvegliato dell'IA nel momento applicativo della legge (e del diritto in generale).

Considerata dunque la complessità delle questioni che il tema racchiude, in questa sede si ritiene opportuno limitare l'analisi ad alcuni dei profili, di matrice costituzionale e di natura pregiudiziale, che esso pone. Tali aspetti infatti precedono, sul piano logico-giuridico, le problematiche inerenti alla "calcolabilità" del diritto nel caso concreto mediante l'impiego dell'IA e alla possibilità tecnica di una pronuncia "robotica". Parallelamente, non si ritiene neanche di entrare nella questione tecnica, a dir poco complessa, del tipo di sistema esperto (*ruled-based* o *machine learning*, etc.) che si potrebbe utilizzare per una simile applicazione dell'IA, pur nella consapevolezza che tale scelta non sia di poco conto. Per il presente lavoro, si assume quindi come premessa di lavoro l'idea di un'IA *comunque* in grado di operare un processo di sussunzione di una fattispecie concreta all'interno di una astratta, attraverso l'elaborazione e l'analisi di grandi quantità di dati normativi, giurisprudenziali e di fatto (c.d. *big data*).

L'indagine, così inquadrata, si focalizzerà sul potenziale impatto dell'IA sui principi cardine del potere giudiziario sanciti dalla Costituzione italiana e sulla misura in cui tale impatto possa essere considerato compatibile con essi. Queste prime riflessioni si propongono, peraltro, di evidenziare la stratificazione e l'interdipendenza dei piani di analisi (giuridica, tecnica ed etica) che caratterizzano qualsiasi disamina sull'automazione della decisione giurisdizionale, anche limitatamente alla prospettiva costituzionale qui adottata.

2. Costituzione, principio antropomorfico e funzioni giurisdizionali

Al fine di orientarsi in questa complessità concettuale, si reputa opportuno muovere dalle recenti

5. Il tema (o, forse, il mito) della calcolabilità del diritto, assai suggestivo, risale alle teorizzazioni di Gottfried Wilhelm von Leibniz; per una ricostruzione del suo pensiero e della sua "eredità" nel XIX secolo v. l'ampia ricostruzione di Triggiano 2013, p. 105 ss.
6. Il punto, tra gli altri, è colto e tradotto in termini chiarissimi da Groppi 2020, p. 679, secondo la quale "Se la democrazia è il potere visibile, secondo la famosa espressione di Norberto Bobbio, questi nuovi strumenti operano invece nell'oscurità e nel segreto degli algoritmi contenuti nei software, incomprensibili per i non addetti ai lavori e spesso di difficile accesso, anche perché coperti dalle norme sulla proprietà industriale. […] Veri e propri poteri invisibili, di fronte ai quali il rischio di quella che è stata definita 'dittatura algoritmica' si fa effettivo".

acquisizioni del diritto amministrativo, ambito che per primo si è confrontato con lo scenario delle decisioni automatizzate, affrontando alcune delle questioni di compatibilità costituzionale che esso solleva. Non è casuale, infatti, che il dibattito costituzionalistico sul tema[7] – sorto in una fase fisiologicamente priva di una legislazione e di una giurisprudenza specificamente dedicate – abbia tratto alimento, almeno inizialmente, proprio da quella esperienza settoriale, ma "contigua".

Per riassumere, nel diritto amministrativo sono emersi principî – di matrice prevalentemente pretoria, giacché necessitati dagli odierni processi di *digital enhancement* delle pubbliche amministrazioni, ad oggi, non puntualmente disciplinati dalla legge – riguardanti la cosiddetta "amministrazione algoritmica", la sua fisionomia e in particolare il regime delle tutele giurisdizionali nei confronti dei provvedimenti da essa adottati. L'obiettivo primario di quella giurisprudenza, lo si intuisce subito, è assicurare che questa modalità operativa della PA sia conforme a quei principî costituzionali (legalità, buon andamento, imparzialità, eguaglianza) e legislativi (giusto procedimento, trasparenza, tempestività, proporzionalità) che guidano la gestione degli interessi pubblici, garantendo al contempo tutele procedurali e giurisdizionali (artt. 24, 103, 113 Cost.) ai cittadini interessati da provvedimenti amministrativi algoritmici: del resto, la vera sfida posta dall'IA in quell'ambito è consistita (e consiste tuttora) nel rendere effettivi tali principî e garanzie rispetto a procedure amministrative che sono state automatizzate dalla PA nel silenzio del legislatore su quello specifico profilo.

Benché con vistose oscillazioni[8], la giustizia amministrativa ha tentato di definire questo fenomeno – inteso correttamente, in dottrina, come "una mutazione cognitiva e antropologica [che] genera una nuova forma di 'potere'"[9] –, alla luce dei principî citati e delle norme sovranazionali allora vigenti (*id est* il solo art. 22 GDPR[10]), individuando alcune imprescindibili condizioni di compatibilità costituzionale (e di legalità) dell'amministrazione digitale algoritmica, quali: (*i*) la conoscibilità *ex ante* dell'utilizzo di strumenti di IA (e delle logiche interne a quest'ultimo) da parte del destinatario del provvedimento automatizzato, (*ii*) la necessità di prevedere un intervento umano, anche solo correttivo, nell'ambito del processo decisionale ("*human in the loop*"), (*iii*) la comprensibilità umana della motivazione del provvedimento così determinato, e (*iv*) la tutela del principio di non discriminazione nella conformazione degli interessi curati dall'amministrazione[11].

In questo quadro stupisce, però, la mancata esplicita analisi, da parte del giudice amministrativo, del rapporto tra amministrazione algoritmica e principio di legalità sostanziale, specialmente riguardo ai requisiti che la norma di legge dovrebbe soddisfare per autorizzare la PA a utilizzare forme di IA in sostituzione dell'azione umana. Come si è tentato di argomentare altrove[12], questa reticenza del giudice amministrativo potrebbe celare la sua consapevolezza circa l'attuale mancanza di solide basi legislative nazionali[13] che prevedano

7. Per tale dibattito v. *supra* nota 3.
8. Il riferimento è alle seguenti pronunce del Giudice amministrativo (tutte consultabili su *giustizia-amministrativa.it*): T.A.R. Lazio, Roma, sez. III-*bis*, sent. nn. 3769/2017, 9227/2018, 10964/2019, nonché Cons. St., sentt. 8 aprile 2019, n. 2270, 13 dicembre 2019 n. 8472/2019 e 4 febbraio 2020, n. 881.
9. Così Simoncini 2020, p. 3.
10. Cfr. Regolamento (UE) 2016/679; in particolare, sull'art. 22 cit. v. le considerazioni di Martire 2022, p. 419 ss.
11. Su questi principî v. la ricostruzione, effettuata alla luce della citata giurisprudenza amministrativa, di Simoncini 2020, p. 19 ss., il quale enuclea dai medesimi una complessiva "*constitutional rule of technology*"; l'A., peraltro, osserva che, in questa materia, il diritto giurisprudenziale italiano ha fatto "un uso dei principi costituzionali nazionali e della Convenzione Europea dei diritti dell'Uomo, molto più stringente della normativa espressa dal GDPR" (p. 29). Cfr. poi Carloni 2020, p. 273 ss.
12. Al riguardo sia consentito rinviare a Francaviglia 2024, p. 114 ss.
13. Né i problemi posti dal profilo teorico di cui si discute nel testo sembrano essere totalmente risolti dai contenuti del più recente Regolamento (UE) 2024/1689 sull'intelligenza artificiale (c.d. *AI Act*), il quale, pur nell'ambito di un approccio "*risk based*" – incentrato principalmente sulle attività interessate dall'impiego di tale tecnologia e

un'attribuzione generale di tale potere alla PA (ammesso e non concesso che quest'ultima sia sufficiente allo scopo, in luogo di una puntuale previsione di legge per ogni singola funzione delegata alle macchine[14]), con tutte le eventuali conseguenze del caso in ordine al perimetro della sua giurisdizione rispetto a tali fenomeni.

Tuttavia, come evidenziato dagli studiosi del diritto amministrativo, è proprio il principio di legalità che potrebbe – più di altri – sottendere un principio antropomorfico (o di preferenza per l'intervento umano), in base al quale "il conferimento di potere decisionale a un certo apparato implic[a] la riferibilità a un atto intenzionale umano se non diversamente stabilito"[15]. Questo principio, sebbene non esplicitato sul piano normativo, sarebbe infatti sempre implicitamente presente "nei discorsi del diritto amministrativo", intesi come "il contesto istituzionale di riferimento condiviso dagli operatori – legislatori, funzionari, cittadini – di quel linguaggio normativo".

Ora, quanto brevemente ripercorso in relazione alla giurisprudenza amministrativa e al dibattito accademico sulle decisioni amministrative automatizzate si ritiene possa essere impiegato, con i dovuti adattamenti, per analizzare il tema delle decisioni giurisdizionali algoritmiche e per sollevare alcune domande di ricerca: quale sarebbe il fondamento – ancor prima che legale – costituzionale di una simile scelta? E, preliminarmente, è necessario un tale fondamento? Inoltre, le norme costituzionali che attribuiscono il potere giurisdizionale alla magistratura contemplano anch'esse un principio "antropomorfico" o comunque una preferenza per l'intervento umano? Infine, i principî precedentemente illustrati, volti a garantire un'amministrazione algoritmica "costituzionalmente orientata", sono estendibili per analogia a un'automatizzazione algoritmica delle funzioni giurisdizionali e sufficienti a rendere quest'ultima un'evoluzione compatibile con la Costituzione?

Le questioni che ci siamo posti rivelano come l'idea di una giustizia gestita da *robot* sollevi problematiche considerevoli, di ordine giuridico e costituzionale *in primis*, che precedono le pur complesse sfide tecniche.

Nel merito, si potrebbe obiettare che le norme costituzionali, essendo il risultato di un processo politico, sono suscettibili di modifica e che si potrebbe quindi risolvere le questioni accennate attraverso una revisione del vigente assetto costituzionale. Tuttavia, questa prospettiva rischia di non tenere in debita considerazione alcuni limiti intrinseci e strutturali del ruolo della giurisdizione all'interno dello Stato costituzionale, limiti che non sarebbero superabili neanche mediante una revisione della Costituzione.

Analizzando da vicino le domande precedentemente formulate, si cercherà di argomentare quest'ultimo punto.

Per quanto concerne l'esistenza e la necessità di un fondamento legale e costituzionale per una giustizia algoritmica (o "robotica"), le prime due domande poste hanno una funzione chiaramente retorica: una qualche forma di "copertura costituzionale" del potere di delegare a un algoritmo la risoluzione di una controversia giuridica con autorità di giudicato è infatti imprescindibile in quanto inerente a una funzione fondamentale dello Stato e potenzialmente idonea a incidere sull'effettività della tutela dei diritti soggettivi e degli interessi legittimi (e, quindi, sulla stessa forma di Stato); ciononostante, tale copertura si presenta al contempo difficilmente realizzabile, stante le evidenti difficoltà – teoriche e pratiche – di considerare un algoritmo come un centro di imputazione di situazioni giuridiche soggettive, tra cui la titolarità di funzioni, poteri, facoltà e responsabilità[16].

non tanto sui soggetti che la utilizzano (nei confronti di terzi) –, muove comunque verso un irrobustimento delle garanzie dei diritti fondamenti coinvolti o interessati da processi decisionali automatizzati di pertinenza di pubblici poteri, e più precisamente di quei principî già individuati dal giudice amministrativo in Italia e costituenti diretta espressione dello Stato di diritto costituzionale (imparzialità, eguaglianza, obbligo di motivazione, trasparenza, ecc.).

14. Su questi aspetti, e sul tema in generale, cfr. l'analisi di Civitarese Matteucci 2019.

15. *Ivi*, pp. 21-22.

16. Né, nella Costituzione repubblicana, è appena il caso di notarlo, si rinviene in capo al corpo magistratuale – né sembra possibile attribuirgli – alcun potere (para-normativo) di delegare a una macchina l'applicazione della legge.

In relazione a quest'ultimo punto, si osserva infatti che proprio il principio costituzionale dell'esclusiva soggezione del giudice alla legge (art. 101 Cost.) postula un rapporto diretto tra il giudice e la norma, che non ammette l'interposizione di elementi esterni o meccanici capaci di sostituire, anche parzialmente, l'elemento umano nel processo di applicazione del diritto[17]. In tal senso, si potrebbe affermare che il legame tra giudice e legge sia immediato e reciproco: se il primo è soggetto unicamente alla seconda, si deve osservare come quest'ultima, per essere validamente applicata, necessiti del secondo, e più precisamente della sua natura umana.

Del resto, la natura umana del giudice – e quindi l'idoneità di quest'ultimo ad essere a sua volta un soggetto giuridico – non solo costituisce il presupposto logico dei requisiti costituzionali della terzietà e indipendenza, ma conferisce altresì concretezza al particolare regime di responsabilità giuridica che discende dall'esercizio della funzione giurisdizionale (come del resto, e più in generale, è affermato, per qualsiasi altra funzione pubblica, dall'art. 28 Cost.).

Un accesso dei cittadini alla giustizia affidato *esclusivamente* a tecnologie intelligenti – e quindi privo della mediazione di un corpo di magistrati "in carne e ossa" – non solo non garantirebbe *ex se* maggiore efficienza o terzietà, ma anzi rappresenterebbe un filtro strutturalmente incline a rendere opachi sia i percorsi argomentativi della decisione automatizzata, sia i soggetti cui attribuirne la responsabilità. Rispetto a tale prospettiva, l'art. 101 Cost. appare dunque come un limite invalicabile.

Se quanto osservato ben può rappresentare una risposta ai primi due quesiti che più sopra si sono sollevati, occorre ora soffermarsi sul terzo, che d'altro canto è logicamente connesso ai precedenti.

Al riguardo, è da osservare come il testo costituzionale presenti numerosi indizi di una concezione intrinsecamente "antropomorfa" delle funzioni giurisdizionali: dalla possibilità che cittadini esterni al corpo magistratuale partecipino all'attività giudiziaria di determinate sezioni degli uffici giudiziari (art. 102 Cost.), alle garanzie di difesa accordate al singolo magistrato in alcuni procedimenti davanti al CSM (art. 107 Cost.), fino alla previsione che le nomine dei magistrati avvengano per concorso (art. 106 Cost.).

Ma tale preferenza per l'elemento umano non dipende unicamente dalle modalità di accesso alla professione di magistrato e dalla tipologia di responsabilità connesse al suo svolgimento. Sembra infatti possibile affermare che il principio di esclusiva soggezione del giudice alla legge presupponga la natura umana del magistrato come elemento imprescindibile (sebbene spesso dato per scontato) della stessa *attività interpretativa* – sia del diritto che dei fatti – che esso è chiamato a compiere nell'ambito di un giudizio, specie allorché il caso controverso richieda all'ordinamento giuridico una risposta di carattere "evolutivo"[18]. Si pensi, a titolo di semplice riscontro sistematico, a quelle disposizioni contenute nei codici di procedura che collegano la natura umana del magistrato alla dinamica processuale stessa, laddove la valutazione delle prove nel rito civile – così come del comportamento delle parti – è ancorata al canone del "prudente apprezzamento" (art. 116 c.p.c.)[19].

17. Al riguardo cfr. Frosini 1977, p. 99 secondo il quale "lo stesso interprete è innestato nell'organismo storico dell'ordinamento, e rappresenta anzi un elemento funzionale della sua logica obbiettiva, a cui non è concepibile che si possa opporre una logica soggettiva diversa dell'interprete stesso; quella del giudice è, infatti, un'azione obbiettivata, che si intesse con le altre nel procedimento, e che fa da tramite fra la struttura della norma legislativa (l'azione come fu obbiettivata ed esemplata dalla legge) e le nuove azioni che ne conseguiranno".

18. Il tema dell'evoluzione della legge, ovvero della possibilità di una sua interpretazione evolutiva, è risalente; per esso si v. il contrasto dottrinario tra Betti 1949, p. 34 ss., il quale ammetteva tale possibilità per la legge e Romano 1947/2013, p. 701 ss., il quale, invece, riferiva tale eventualità all'ordinamento in sé considerato.

19. Su questo profilo v. le considerazioni di Pajno 2022, p. 223 ss.; in ambito penale il tema dell'apprezzamento da parte del giudice del materiale probatorio (che, di norma, si forma in contraddittorio fra le parti e nel corso del dibattimento) è ancora più delicato giacché risulta strettamente connesso al superamento di quel ragionevole dubbio, solo oltre il quale è possibile giudicare l'imputato colpevole dei reati ascrittigli (v. artt. 192, 533, 546, co. 1, 606 c.p.p.); su quest'ultimo punto v. le considerazioni di Carlizzi 2018, p. 5, secondo il quale è proprio quella connessione tra l'autonomia valutativa del giudice penale e le regole processuali per la ricostruzione

Sarebbe ipotizzabile adattare questo elemento fondamentale della concreta dinamica del processo civile a un processo giurisdizionale integralmente automatizzato?

Proprio disposizioni di carattere processuale come l'art. 116 c.p.c., al pari delle altre norme costituzionali precedentemente richiamate, esprimono – per quanto indirettamente – un chiaro principio antropomorfico, analogo a quello che, con riferimento alle pubbliche amministrazioni, deriva dal principio di legalità, e tuttavia *diverso* per intensità e rigore[20]. Rispetto a quanto riscontrato nell'ambito della c.d. amministrazione algoritmica, la declinazione costituzionale del principio antropomorfico in relazione alle funzioni giurisdizionali non pare, infatti, ammettere deroghe o "aperture condizionate"; in base al principio in parola, il potere di applicare la legge pertiene unicamente a un giudice-persona fisica, designato secondo i meccanismi e le garanzie previste dalla Carta costituzionale (di cui agli articoli 25, 101, 107 e 108 della Costituzione), escludendo qualsiasi interferenza decisiva (o sostituzione) da parte di macchine o altri apparati, né l'applicazione all'organizzazione delle funzioni giurisdizionali dei principî precedentemente richiamati per la c.d. amministrazione algoritmica sembra rappresentare elemento sufficiente a consentire di aggirare i limiti che (implicitamente) emergono dal testo costituzionale[21].

3. Intelligenza artificiale e il dibattito sull'interpretazione giuridica: nuove premesse e nuovi problemi

Alla luce di quanto sin qui osservato, ci si può rendere conto di come il tema dell'impiego dell'IA nell'ambito delle funzioni giurisdizionali possa impattare non solo sul ruolo del giudice, ma vieppiù sull'esercizio in sé della funzione giurisdizionale e segnatamente sull'attività interpretativa, che di quest'ultima rappresenta uno dei principali vettori.

Da questa prospettiva, l'avanzamento tecnologico in materia di IA ha avuto il merito di gettare una nuova luce su importanti e risalenti problemi teorico-giuridici, spingendoci a riflettere sul significato profondo di alcuni concetti fondamentali dell'attività giurisdizionale, e in particolare su quello di "interpretazione giuridica"[22]. Non solo,

del caso in giudizio che garantiscono "la giustizia della decisione penale, cioè la sua aderenza sia alle particolarità del caso sia alle aspettative di garanzia dell'imputato"; nonché v. Quattrocolo 2019, p. 1748. Il profilo di cui discute nel testo si presenta, peraltro, anche per l'applicazione di quelle norme (processuali e non) che fanno riferimento a concetti astratti o generali (per es., il buon costume), rimessi spesso alla sensibilità del giudicante; su quest'ultimo profilo cfr. De Renzis 2019, p. 147.

20. Vale peraltro notare come, nell'ambito degli studi amministrativistici, esistano anche letture particolarmente rigorose del principio antropomorfico o di preferenza dell'intervento umano, tali da concepire una vera e propria "riserva di umanità". Per quest'ultimo concetto v. Gallone 2023, spec. pp. 38-66, secondo il quale la sfera di azione della PA è "inderogabilmente sottratta all'automazione e riservata all'uomo" e ciò si traduce in un divieto di rango super-primario "di prevedere modalità di esercizio della capacità autoritativa totalmente automatizzate". Non è questa la sede per entrare nel merito di questa teoria, che appare fondata su di una lettura assolutizzante del principio di preferenza antropica che non sembra del tutto rispondente a una lettura attualizzata del quadro normativo costituzionale relativo alla P.A.; per un concezione diversa di riserva di umanità, parzialmente coincidente con quella di legge, sia consentito rinviare alle argomentazioni espresse in Francaviglia 2024, pp. 123-124; sul medesimo tema cfr. anche le considerazioni di Casonato 2019, p. 177 ss., spec. p. 180.

21. Principî, peraltro, parzialmente coincidenti con quelli sanciti, in via generale, dal c.d. *Ai Act*, oltreché con quelli elaborati ancor prima dalla Commissione europea per l'efficienza della Giustizia (CEPEJ) nell'ambito dell'adozione della "Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari", del 3 dicembre 2018.

22. Sul tema, colossale, dell'interpretazione v. le classiche pagine di Betti 1949, p. 3 ss., secondo il quale "l'interpretazione che interessa il diritto è un'attività volta a riconoscere e a ricostruire il significato da attribuire, nell'orbita di un ordine giuridico, a forme rappresentative, che sono fonti di valutazioni giuridiche, o che di siffatte valutazioni costituiscono l'oggetto. […] il problema che caratterizza questo tipo di interpretazione è il problema dell'intendere per agire o, comunque, per decidere". Il rapporto tra attività interpretativa e funzione giurisdizionale si fa, peraltro, più intenso laddove si accede all'impostazione kelseniana che arriva a fondere i

esso richiama anche il distinto problema – chiaramente connesso a quello della natura e dei limiti dell'attività interpretativa – del tasso di razionalità (o di certezza[23]) che dovrebbe caratterizzare l'esperienza giuridica nell'attuale contesto storico e socio-economico.

In altre parole, la sfida dell'IA, offrendo una nuova prospettiva sulla distinzione tra disposizione e norma[24] (o, più precisamente, tra norma generale e quella applicata al caso specifico), tocca senz'altro il rapporto tra il giudice e la legge, con evidenti implicazioni sugli archetipi classici del costituzionalismo liberale, tra cui spicca la separazione dei poteri e la persistente tensione tra potere legislativo e potere giudiziario. Proprio a quest'ultimo riguardo, vale peraltro ricordare come proprio il rapporto tra legislazione e giurisdizione sia stato oggetto di un intenso, e assai longevo, dibattito costituzionalistico, il quale si è inevitabilmente focalizzato sul ruolo del giudice, e in particolare sull'interpretazione giuridica operata da questi[25].

Tuttavia si deve escludere che il tema dell'intelligenza artificiale in ambito giuridico impatti in modo diretto su tale dibattito (e sul problema teorico-giuridico che ne è oggetto). In realtà, i due piani speculativi, sebbene capaci di influenzarsi a vicenda, seguono percorsi paralleli, basandosi su presupposti radicalmente differenti proprio con riferimento al soggetto che deve (o dovrebbe) interpretare il diritto: da un lato un giudice in carne e ossa, dall'altro una forma di intelligenza artificiale.

Ne consegue che le problematiche legate allo spazio da riconoscere al fattore ermeneutico della precomprensione[26] nell'ambito dell'interpretazione del diritto da parte del giudice-persona devono essere riformulate, in questo diverso contesto, come interrogativi sulle scelte (indirettamente ermeneutiche) da compiere nella progettazione dell'intelligenza artificiale destinata al calcolo decisionale, o, ancora più a monte, sulla natura dell'intelligenza e dei processi logici richiesti dalla Costituzione non solo per l'esercizio delle funzioni giurisdizionali, ma per la garanzia di quanto in essa previsto. Ed è proprio quest'ultimo profilo che dischiude un'ulteriore orizzonte di analisi, concernente la stessa interpretazione costituzionale.

4. Intelligenza artificiale, interpretazione costituzionale e garanzia dei diritti fondamentali

L'analisi dei limiti dell'IA in ordine al compimento di attività giurisdizionali, e segnatamente di quella interpretativa, finisce per investire profili di natura strettamente costituzionale laddove si ponga mente alle ben note dinamiche involutive che, negli

due concetti e a tradurre l'interpretazione giudiziale in un "giudizio prescrittivo" e, dunque, in norma del caso concreto (né vera, né falsa, ma solo valida o invalida alla luce del livello normativo superiore): così per Kelsen 1960/1966, p. 387, secondo il quale "nell'applicazione del diritto da parte di un organo giuridico l'interpretazione teorica del diritto da applicare si collega con un atto di volontà, in cui l'organo incaricato dell'applicazione del diritto compie una scelta fra le possibilità rilevate dall'interpretazione teorica. Con quest'atto o si produce una norma di grado inferiore o si esegue un atto coercitivo previsto dalla norma da applicare. Grazie a quest'atto di volontà, l'interpretazione giuridica dell'organo che applica il diritto si distingue da ogni altra interpretazione, particolarmente dall'interpretazione del diritto da parte della scienza giuridica". I problemi teorici e definitori dell'interpretazione giuridica (e delle sue diverse tipologie-metodologie) sono molteplici e vastissima è la letteratura in argomento; al riguardo, senza pretesa di completezza e con riferimento al dibattito costituzionalistico più recente, si v. per tutti le (parzialmente) diverse impostazioni di Modugno 2012, e di Pace 2001, p. 38 ss.

23. Sul punto v. da ultimo le considerazioni di Luciani 2023, *passim*.
24. Si tratta di una distinzione classica della dottrina costituzionalistica italiana che si deve, com'è noto, a Crisafulli 1964, p. 195 ss.
25. Si tratta di una discussione ancora aperta, nell'ambito della quale sono emerse diverse letture del problema, a seconda che si riconosca o meno una certa autonomia creativa al giudice nell'individuare il significato normativo da applicare al caso concreto. Non essendo questa la sede per entrare in tale impegnativo dibattito, cfr., per tutti, le diverse posizioni, rispettivamente, di Pinelli 2016, p. 8 ss., Pinelli 2019, p. 549 ss., Luciani 2016, p. 391, spec. p. 401 ss., nonché Luciani 2023, spec. p. 161 ss.
26. Sul concetto di precomprensione il riferimento obbligatorio è a Gadamer 1960/2000, p. 551 ss.

ultimi decenni, stanno caratterizzando la produzione normativa all'interno dello Stato costituzionale: sebbene il fenomeno della "crisi della legge" abbia origini risalenti e assunto molteplici accezioni e sfumature[27], oggi si è certamente di fronte a un ulteriore processo di deterioramento del paradigma legale, tale da rendere sempre più importante il momento interpretativo e di ricostruzione dei materiali normativi rispetto al caso di specie.

Muovendo dalla concezione kelseniana che invita a "evitare con la massima cura possibile la finzione secondo cui una norma giuridica ammette sempre e soltanto un'interpretazione, quella 'esatta' (*richtig*)"[28], è stato dunque lucidamente ricordato che, in un contesto ordinamentale di questo tipo, l'obbiettivo del giudice non può essere quello di cogliere (e affermare) una "verità", eterna e immutabile, dell'ordinamento giuridico, ma quello – forse più limitato, ma anche più concreto – di "prestare collaborazione affinché il significato del diritto fondamentale cessi di essere controverso" (Corte cost., sent. n. 49/2015)[29]. E, per quanto possa sembrare paradossale, proprio questa collaborazione si nutre, tra gli altri elementi, della capacità del singolo giudice di interrogarsi sulla portata normativa della legge che è chiamato ad applicare al caso concreto, soprattutto in relazione alla sua conformità alla Costituzione; una capacità che non sembra caratterizzare i modelli di IA, persino di quelli più complessi e raffinati.

Questi ultimi, infatti, operano sulla base di processi non sempre accessibili alla logica umana e comunque risultano "leibnizianamente" orientati – su fondamenti statistici o probabilistici – a individuare, in ogni circostanza, un'unica soluzione "corretta" o "esatta" rispetto al caso specifico ("calcolata" sulla base dei dati di cui la macchina dispone). La problematizzazione dubitativa e dialettica del caso concreto ("*to argue a case*"), che precede la sua risoluzione ("*to solve a case*") e che può persino portare alla sospensione dell'attività giurisdizionale (per es., per sollevare incidenti processuali di natura pregiudiziale, quale è quello di costituzionalità della norma di legge rilevante), rappresenta invece una eventualità propria e *tipica* della mente umana, come tale insostituibile nella logica applicativa della stessa Costituzione.

Del resto, questa "abilità" dell'intelligenza umana di dubitare, quale elemento essenziale del processo ermeneutico nell'ambito dello Stato costituzionale, non solo costituisce la migliore confutazione dell'esistenza di un'*unica* norma "corretta" (e quindi "vera") per il caso di specie, ma trova altresì un riscontro indiretto ma significativo nella stessa previsione costituzionale in base alla quale ogni provvedimento giurisdizionale deve essere motivato (art. 111, co. 6, Cost.): proprio perché un'interpretazione "corretta" (*rectius*: "vera") è gnoseologicamente inattingibile, ciò che può realmente essere oggetto di verifica – ai fini sia della legittimità della decisione, sia della sua legittimazione/accettazione da parte dei consociati – è solo "l'adeguatezza del ragionamento"[30] svolto dall'organo giudicante rispetto alle premesse (di fatto e di diritto) offerte dal caso concreto e tale controllo passa necessariamente per la motivazione espressa (e comprensibile) del provvedimento giurisdizionale quale luogo dove poter ricostruire *ex post* la *logica* della decisione presa.

Da questa prospettiva, abbandonare l'idea che la *certezza del diritto* coincida unicamente con la *certezza della legge* rappresenta, allora, un passaggio teorico cruciale per comprendere il *perché* la Costituzione repubblicana abbia declinato, in relazione al potere giudiziario, il suddetto principio antropomorfico in modo così rigoroso. Tale impostazione risulta, infatti, strettamente funzionale al corretto sviluppo degli assetti interpretativi della Costituzione stessa e in particolare di quelli concernenti i diritti fondamentali.

Infatti, in un modello di controllo di costituzionalità accentrato, tale progresso non può ignorare gli sviluppi interpretativi che, grazie al meccanismo della questione incidentale, provengono dai singoli magistrati e che dipendono strettamente dalla loro abilità di dubitare, alla luce dei dettami costituzionali, dell'*adeguatezza* di un'interpretazione che, attraverso la legge, sono tenuti ad applicare al caso concreto. In altre parole, proprio il "dubbio

27. Di tale circostanza ce ne dà un saggio significativo Pinelli 2019, p. 552.

28. Così Kelsen 1960/1966, p. 286.

29. Valorizza questa pronuncia nel senso indicato nel testo Pinelli 2019, p. 558 ss.

30. *Ibidem*.

interpretativo", innescando percorsi argomentativi inediti, non solo consente al giudice di adeguare le risposte dell'ordinamento al caso di specie, ma permette allo stesso giudice costituzionale di trovare nuovi assetti interpretativi, anche di tipo evolutivo, con riguardo al testo della Costituzione, onde massimizzarne la precettività.

Se questa analisi è corretta, è allora possibile ricollegare le ragioni profonde di questo approccio antropomorfico del costituente in relazione al potere giudiziario alla tensione – sottaciuta dalla Costituzione ma in essa immanente – tra la naturale incertezza della legge (o meglio: dei suoi risultati applicativi) e l'esigenza di garantire un certo grado di certezza del diritto, intesa quest'ultima non come immutabilità statica dell'ordinamento giuridico, bensì nel preciso significato di "una primaria esigenza di diritto costituzionale che sia raggiunto uno stabile assetto interpretativo sui diritti fondamentali" (così Corte cost., sent. cit.).

In questo contesto, emergono dunque con particolare nitore tutti i limiti di una delega integrale di funzioni giurisdizionali a forme di intelligenza artificiale: il primo e decisivo ordine di problemi, infatti, attiene proprio alla difficoltà di mantenere intatte quelle dinamiche evolutive e di garanzia costituzionale, tipiche dello Stato costituzionale (specie per gli ordinamenti di c.d. *civil law*), che si celano dietro l'attività interpretativa di ogni singolo giudice.

Solo la mente umana, al momento, è in grado di garantire la possibilità di interpretazioni adeguatrici o evolutive (dell'ordinamento giuridico e della Costituzione), mentre l'IA, essendo letteralmente costruita su asset di dati riguardanti il passato (ed essendo concepita per apprendere solo sulla base di essi)[31], risulta strutturalmente orientata in modo retrospettivo: ogni possibile soluzione avrà come modello solo precedenti decisioni, con un evidente effetto di irrigidimento e di impoverimento del c.d. diritto vivente (inteso quest'ultimo in senso lato)[32].

Non solo. Tale effetto di "pietrificazione" dell'ordinamento si coniuga con i concorrenti rischi –già evidenziati nella giurisprudenza amministrativa più sopra richiamata – di incomprensibilità delle motivazioni della decisione algoritmica, specie sul piano della verificabilità del percorso logico seguito dalla macchina e dell'adeguatezza di questo al caso di specie, con evidente sovvertimento di quella logica costituzionale cui il concreto funzionamento del potere giudiziario deve sottendere e di cui più sopra si è fatto cenno.

Da questa angolazione, diviene allora chiaro come la questione della pronuncia giurisdizionale algoritmica non sia facilmente gestibile in prospettiva futura da un legislatore costituzionale, poiché una sua introduzione sul piano del diritto costituzionale positivo influenzerebbe non tanto il modo di operare della magistratura, quanto il suo ruolo e la sua funzione all'interno dello Stato costituzionale, specialmente in relazione all'effettivo funzionamento del giudizio di costituzionalità delle leggi. Si tratterebbe di un'operazione più vicina a una vera e propria palingenesi costituzionale – suscettibile di interessare, forse, gli stessi principî supremi dell'ordinamento costituzionale – che a una semplice modifica tecnica, con esiti dubbi riguardo alla conservazione di un'interpretazione dei diritti fondamentali che, pur stabile, permetta una sua fisiologica evoluzione attraverso il sindacato accentrato di costituzionalità.

31. In questa sede non si ritiene necessario richiamare (dandoli per scontato) i molteplici limiti tecnici che oggi ancora si frappongono a un modello di IA che sia in grado di risolvere una questione giuridica senza tuttavia tradurla in una mera "prospettiva statistica", ottenuta sulla base di un'analisi sintattica dei testi giurisprudenziali e normativi inseriti nell'algoritmo. Sul punto sia consentito rinviare a Francaviglia–La Pegna 2024, p. 181 ss.
32. Al riguardo, cfr. Luciani 2018, p. 86, secondo il quale l'evoluzione degli indirizzi giurisprudenziali risponde "ai bisogni umani regolando rapporti corrispondentemente alle esigenze sociali del momento storico". Dello stesso avviso è Sciacca 2023, p. 8 secondo il quale quello in esame rappresenterebbe "uno dei tanti paradossi dell'innovazione tecnologica, la quale – consacrando che la legge si fonda ormai più sulla *quantitas anteatta*, piuttosto che sull'*auctoritas* – diverrebbe un formidabile araldo della conservazione e del rafforzamento delle tendenze maggioritarie. Si realizzerebbe per tale via una sorta di pietrificazione del tempo attraverso l'affermazione di un tempo virtuale che, per predire il futuro possibile, nel presente valorizza il passato, rafforzando l'ideologia a scapito della utopia, ovvero del futuro stesso".

5. Possibili impieghi dell'IA nell'ambito delle funzioni giurisdizionali: una questione di metodo

Quelle finora delineate costituiscono le prime difficoltà di ordine strettamente costituzionale che la decisione robotica pare innescare, cui si devono aggiungere quelle derivanti dal più ampio contesto dell'integrazione dell'ordinamento interno con la sfera sovranazionale e che si focalizzano, tra gli altri profili, sulla imprescindibile trasparenza "interna" dell'algoritmo cui verrebbero demandate funzioni giurisdizionali, sulla intellegibilità dei relativi provvedimenti decisori da parte dei soggetti destinatari e sulla salvaguardia della riservatezza nella gestione ed elaborazione automatizzata di dati giudiziari.

Al netto di ciò, però, sarebbe miope e irrealistico negare qualsiasi beneficio da un utilizzo accorto dell'intelligenza artificiale in alcune fasi del lavoro del giudice, specie quelle di tipo istruttorio: rispetto a contenziosi particolarmente complessi (sia sotto il profilo fattuale, che giuridico) sul giudice-persona grava, infatti, un non secondario onere di ordinare e gestire rilevanti quantità di dati di fatto e giuridici[33]; non solo, l'IA potrebbe rappresentare uno strumento chiave anche rispetto all'uniformità applicativa del diritto oggettivo (specie laddove non residuino ragioni di giuridiche – in ultima analisi connesse al superiore quadro costituzionale e sovranazionale – per il superamento di un determinato assetto interpretativo): in questo senso, l'impiego di forme di IA per ricostruire l'esatta portata di un determinato orientamento giurisprudenziale coadiuverebbe non poco il giudice nel non incorrere nei cc.dd. "contrasti inconsapevoli"[34], contribuendo così a garantire una maggiore (sebbene sempre relativa) prevedibilità delle decisioni.

Riguardo a questa ipotesi di utilizzo, parte della dottrina ha, peraltro, formulato proposte abbastanza puntuali, come quella, per esempio, di configurare la soluzione elaborata dalla macchina nei termini di un "parere obbligatorio" non vincolante, rispetto al quale il giudice può discostarsi motivando in sentenza il proprio diverso opinare[35].

Senza voler qui entrare nel merito di siffatte proposte, si deve comunque riconoscere che l'impiego dell'IA in attività ausiliarie e istruttorie di questo tipo (parte delle quali, non a caso, oggi vengono delegate ad esseri umani, nell'ambito del c.d. Ufficio per il processo) può rappresentare senz'altro un notevole salto di qualità nell'esercizio della funzione giurisdizionale, con effetti evidenti sui

33. Cfr. Libertini–Maugeri–Vincenti 2021, secondo i quali "si deve infatti considerare che oggi, nell'affrontare in modo esauriente un singolo caso, che non sia già perfettamente tipizzato e di routine, la quantità di dati potenzialmente influenti sulla decisione [principi di rango costituzionale (che devono tenere conto di una prospettiva di costituzionalità "multi- livello"), fonti formali di varia provenienza, precedenti giurisprudenziali, strumenti di soft law, proposte dottrinali, dati comparatistici (comprensivi dei precedenti stranieri)] è così ampia che l'acquisizione completa della relativa informazione trascende le possibilità di qualsiasi agente umano". A questa lettura, certamente realistica, dell'attuale situazione, Ruffolo 2021, p. 211 ss., osserva appunto che "l'opera dell'algoritmo è molto più veloce e completa nel compulsare il groviglio dei dati normativi come dei precedenti giurisprudenziali".

34. Al riguardo v. Manes 2021, p. 283 ss., che, posta "la necessita di una 'relativizzazione' dei sistemi di decisione algoritmica", sottolinea l'importanza per il giudice di avvalersi di un "*double check* algoritmico", "quale parametro di verifica, a valle, della decisione adottata a monte dal giudice umano, in un percorso che preveda l'utilizzazione dell'algoritmo in funzione tutoria, per limitare la fallibilità della decisione giudiziale, nel quadro della collaborazione uomo-macchina".

35. Per questa proposta v. Ruffolo 2021, p. 210, secondo il quale un meccanismo del genere avrebbe il merito di conciliare "le aspettative di certezza del diritto con quelle di adeguamento interpretativo delle norme alla realtà mutata". Infatti, il giudice umano rimarrebbe sempre "libero di discostarsi dalle previsioni o conclusioni algoritmiche, tanto rilevandone la erroneità quanto motivando una interpretazione evolutiva" necessaria ad un mutato contesto sociale. Una proposta sostanzialmente analoga è formulata anche da Griffi 2019, p. 174 ss.; di portata più limitata, ma forse di impatto pratico maggiore, è poi la proposta di Covelli 2019, p. 132 ss., di delegare all'IA attività endoprocessuali totalmente vincolate, per le quali non residui alcun elemento di discrezionalità.

tempi della giustizia[36]. E non mancano in dottrina coloro che, proprio con riferimento a questa prospettiva, hanno colto l'importanza di superare sia "il rifiuto tecnofobico sia il sogno che la macchina possa immunizzare l'era della complessità dal morbo dell'incertezza", evidenziando la necessità di imboccare una via alternativa, "ispirata all'idea dell'interazione feconda tra l'uomo e il robot"[37].

Una volta, dunque, individuato nella decisione del caso concreto la soglia dinanzi alla quale la tecnologia deve necessariamente arrestarsi per lasciare spazio all'elaborazione umana[38], non sembra vi siano, per la maggior parte degli osservatori, particolari difficoltà teoriche rispetto all'ingresso dell'IA nel settore giustizia quale mero ausilio o strumento conoscitivo. Secondo alcuni, si tratterebbe di conseguire una "predittività mite"[39], giacché consapevole, vigilata, e imperniata su interazioni tra macchina e giudice nell'ambito delle quali la prima sia programmata unicamente per fornire al secondo dati conoscitivi e stimoli per la riflessione, senza creare pressioni indebite circa la decisione da prendere.

Tuttavia, la realizzazione concreta di un'operazione del genere è assai più impervia e rischiosa di quanto possa sembrare. Il rischio più concreto, infatti, è quello di inserire all'interno del processo elementi di deresponsabilizzazione del giudice[40] ovvero strumenti tecnologici in grado di "catturare" la decisione umana[41], specie laddove l'apporto della macchina venga veicolato nella forma di un parere obbligatoriamente prodromico rispetto alla decisione umana.

Si tratta di un profilo critico tenuto bene a mente anche dal diritto sovranazionale, e segnatamente dal c.d. *AI Act*[42], rispetto al quale le soluzioni regolatorie ad oggi prospettate (o in vigore) potrebbero risultare non del tutto efficaci, specie se ad esse

36. Per un quadro aggiornato degli strumenti normativi adottati dal legislatore per ridurre l'irragionevole durata dei processi, specie con riferimento alle iniziative di digitalizzazione del processo, v. Bailo 2024.
37. Così Punzi 2019, p. 328.
38. Cfr. sul punto Donati 2020, p. 442, secondo il quale "l'importante è che il ricorso [all'intelligenza artificiale, ndr.] non sia mai finalizzato a sostituire, ma soltanto a coadiuvare, il decidente umano; in altre parole, la giustizia predittiva non dovrebbe mai oltrepassare la soglia della fase di decisione, fase quest'ultima che deve rimanere integralmente, sotto la sorveglianza umana e, soprattutto, sotto la responsabilità del giudice (posto che la responsabilità incentiva la diligenza)".
39. Per questa locuzione v. Dalfino 2018, p. 385; v. poi Ancona 2018; nonché Sciacca 2023, ult. loc. cit. e ss.
40. Cfr. sul punto Donati 2020, p. 445, il quale evidenzia come "i giudici tendano a 'deresponsabilizzarsi', affidandosi alle 'risposte' fornite dall'algoritmo sia in buona fede, confidando cioè nella validità del medium tecnologico (secondo la deviazione comportamentale del cd. *automation bias*, messa in luce anche dal regolatore eurounitario) sia per superficialità, sia per ragioni di 'giustizia difensiva', ossia per il timore di vedersi esposti a rischi di responsabilità civile per aver disatteso le indicazioni provenienti dal programma". Proprio con riferimento a quest'ultimo profilo v. poi le analoghe considerazioni (critiche) di Manes 2020, p. 557.
41. Il riferimento, chiaramente, è alla c.d. *nudging theory* secondo la quale la c.d. *default option* è quella solitamente preferita dall'uomo; sulle implicazioni giuridiche di tale problema v. l'analisi di Simoncini 2023, p. 16, che sottolinea l'innegabile "plusvalore 'pratico' della scelta suggerita automaticamente dal sistema, rispetto alla quale ci si può discostare, ma a patto di impegnarsi in un notevole sforzo (e rischio) valutativo". Cfr. poi Donati 2020, *passim*; Santosuosso–Sartor 2022, p. 1779; Tuzet 2020, p. 45.
42. Si veda al riguardo l'art. 14, par. 4, lett. b), del citato Regolamento sull'intelligenza artificiale, ai sensi del quale: "Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ('distorsione dell'automazione'), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche".

non si affianchi un'adeguata formazione del corpo magistratuale rispetto ai limiti che i modelli di IA presentano e dunque al corretto utilizzo che di essi deve essere fatto.

Da questa prospettiva emerge allora con chiarezza come i problemi giuridici (oltreché tecnici) che discendono dall'interazione tra macchina e giudice si riducano essenzialmente a una questione di metodo: qualunque impiego – tra quelli costituzionalmente ammissibili – dell'IA nell'ambito delle funzioni giurisdizionali non può, infatti, prescindere da una precisa cornice normativa (e *in primis* legislativa) che, nel rispetto dei principî costituzionali e sovranazionali cui si è fatto cenno più sopra, disciplini in modo olistico l'ingresso dell'IA nelle attività giurisdizionali, investendo tutti gli aspetti a quest'ultime connessi, da quelli tecnici (relativi ai principî da seguire nella progettazione degli strumenti di IA), a quelli strettamente processuali (concernenti le fasi processuali e i limiti entro i quali utilizzare detta tecnologia), sino a quelli attinenti all'organizzazione degli uffici giudiziari e alla formazione dei singoli magistrati.

Un intervento di questo tipo ad oggi è assente, sicché non stupiscono quei tentativi della complessiva macchina della giustizia di darsi comunque delle regole in tema di nuove tecnologie attraverso circolari ministeriali, intese, convenzioni e altri atti sub-primari[43]; senonché tali iniziative, prive di una sufficiente copertura legislativa e senza adeguati meccanismi di trasparenza e controllo, risultano un rischio ancor più elevato per la tenuta del giusto processo e dei diritti fondamentali.

6. Alcune conclusioni alla luce del PNRR: sull'attualità della distinzione tra funzioni giurisdizionali e "servizi relativi alla giustizia"

Quanto finora esposto delinea un orizzonte di notevole complessità e rende congetturale, se non del tutto aleatorio, qualsiasi tentativo di anticipare gli sviluppi dell'ordinamento su questi temi, specialmente in riferimento a possibili iniziative *de iure condendo*.

Ciò che però può essere notato sin d'ora è la permanente utilità della distinzione operata dalla Costituzione tra le funzioni giurisdizionali *tout court*, esercitate dai giudici "in nome del popolo" (art. 101 Cost.) e "governate" dal Consiglio superiore della magistratura, e i "servizi relativi alla giustizia", la cui organizzazione e il cui funzionamento spettano al Ministero della giustizia (art. 110 Cost.).

Tale discrimine è rilevante poiché, da un lato, chiarisce la duplice natura della giustizia – da intendersi sia come funzione sovrana sia come "servizio pubblico" a beneficio dei singoli cittadini –, mentre dall'altro lato ci ricorda che il corretto funzionamento di detto servizio – da intendersi nei termini di un accesso rapido, efficiente e universale alla "prestazione giustizia" – è condizionato dalle iniziative del Governo (nei limiti, ovviamente, del principio di legalità, qualora si tratti di azioni amministrative).

Ebbene, ferma questa distinzione e i distinti ordini di competenze che da essa discendono, non appare casuale che le misure di maggior impatto del PNRR nell'ambito della giustizia riguarderanno quest'ultima nella sua dimensione di servizio pubblico. Per quanto di interesse in questa sede, infatti, gli obiettivi di riduzione dei tempi processuali e di miglioramento, sotto il profilo organizzativo, di tutti servizi di giustizia vengono ancorati, oltre che a significativi progetti di riforma legislativa dei riti (civile, penale e tributario), a un processo di digitalizzazione del "bene-giustizia" e, in particolare, a un marcato potenziamento dei sistemi informatici di gestione dei procedimenti. E la riprova di quanto affermato la si coglie nella consistenza delle risorse finanziarie delineate dal Piano relativamente a quegli aspetti del "servizio giustizia". Ad oggi, dunque, l'impiego dell'intelligenza artificiale nel settore Giustizia sembra essere limitato al rafforzamento dei percorsi – già in atto in Italia da almeno un decennio – di digitalizzazione delle attività "burocratiche" connesse al concreto funzionamento del processo (le quali, in realtà, ne rallentano considerevolmente lo svolgimento); altri utilizzi, più pervasivi, dell'IA non sono invece contemplati dal Piano – né da altri documenti governativi – e ciò conferma la volontà dei decisori politici di digitalizzare, appunto, non la Giustizia in sé (e i suoi protagonisti, giudici e avvocati), ma

43. Cfr. al riguardo le vicende del processo penale telematico (di cui al D.M. n. 217/2023) e della relativa App. Su questi temi v. in particolare le ricostruzioni di Palmieri 2024, p. 445 ss.; Ubertis 2024, p. 439 ss.; nonché Della Torre–Malacarne 2024, p. 287 ss.

esclusivamente le attività non prettamente giurisdizionali ad essa funzionali, siano esse di natura organizzativa ovvero di supporto ai singoli magistrati nell'elaborazione di decisioni tecnicamente e giuridicamente più consapevoli.

Da questo punto di vista, il PNRR costituisce un indicatore qualificato della direzione che si intende imprimere, a livello di indirizzo politico-amministrativo, all'ordinamento giuridico su questo specifico orizzonte.

D'altra parte, però, è bene anche segnalare come la coerenza e l'effettività di tale indirizzo dipendano in larga misura dalla condizione – materiale, ma anche culturale – in cui versano attualmente gli Uffici giudiziari e, in particolare, quei servizi amministrativi che consentono ai singoli magistrati l'espletamento delle loro mansioni. Sicché, ancora una volta, emerge la necessità di interventi normativi che affrontino in modo organico tutte le questioni che l'IA pone sul fronte della giustizia: solo così sarà possibile tradurre tale strumenti in una risorsa per gli operatori del diritto e, soprattutto, per gli utenti del "servizio Giustizia".

Riferimenti bibliografici

M. Ancona (2018), *Verso una giustizia predittiva "mite"*, in "Rivista quadrimestrale per l'innovazione sociale", 2018, n. 2

F. Bailo (2024), *L'irragionevole durata del processo e gli strumenti legislativi per porvi rimedio: dall'implementazione del capitale umano alla digitalizzazione della giustizia*, in "federalismi.it", 2024, n. 27

E. Betti (1949), *Interpretazione della legge e degli atti giuridici (Teoria generale e dogmatica)*, Giuffrè, 1949

A. Carleo (a cura di) (2019), *Decisione robotica*, il Mulino, 2019

G. Carlizzi (2018), *Libero convincimento e ragionevole dubbio nel processo penale. Storia prassi teoria*, Bonomo Editore, 2018

E. Carloni (2020), *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2

S. Civitarese Matteucci (2019), *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in "Diritto pubblico", 2019, n. 5

A. Cerri (2023), *Spunti e riflessioni sull'impiego dell'Intelligenza Artificiale nei procedimenti giuridici*, in "Diritto pubblico", 2023, n. 1

V. Crisafulli (1964), *Disposizione (e norma)*, in "Enciclopedia del diritto", vol. xiii, 1964

M.R. Covelli (2019), *Dall'informatizzazione della giustizia alla decisione robotica? Il giudice di merito*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

A. D'Aloia (2022), *Intelligenza artificiale, società algoritmica, dimensione giuridica. Lavori in corso*, in "Quaderni costituzionali", 2022, n. 3

F. Dalfino (2018), *Creatività e creazionismo, prevedibilità e predittività*, in "Foro italiano", 2018, n. 5

L. De Renzis (2019), *Primi passi nel mondo della giustizia "high tech": la decisione in un corpo a corpo virtuale fra tecnologia e umanità*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

J. Della Torre, A. Malacarne (2024), *Riforma Cartabia e digitalizzazione della giustizia penale*, in "Rivista italiana di informatica e diritto", 2024, n. 2

F. Donati (2020), *Intelligenza artificiale e giustizia*, in "Rivista AIC", 2020, n. 1

L. Durst (2024), *Diritto e predittività. Spunti introduttivi in tema di sistemi decisori automatizzati*, in F. Fabrizzi, L. Durst (a cura di), "Controllo e predittività. Le nuove frontiere del costituzionalismo nell'era dell'algoritmo", Editoriale Scientifica, 2024

F. Fabrizzi, L. Durst (a cura di) (2024), *Controllo e predittività. Le nuove frontiere del costituzionalismo nell'era dell'algoritmo*, Editoriale Scientifica, 2024

M. Francaviglia (2024), *L'intelligenza artificiale nell'attività amministrativa: principî e garanzie costituzionali nel passaggio dalla regula agendi alla regola algoritmica*, in "federalismi.it", 2024, n. 17

M. Francaviglia, A. La Pegna (2024), *Le funzioni giurisdizionali*, in M.E. Bucalo, M. Caporale, A. Sterpa (a cura di), "Diritto pubblico di internet", Editoriale Scientifica, 2024

V. Frosini (1977), *La struttura del diritto*, Giuffrè, 1977

H.G. Gadamer (1960/2000), *Wahrheit und Methode* (1960), trad. it. *Verità e metodo*, Bompiani, 2000

G. Gallone (2023), *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Cedam, 2023

F.P. Griffi (2019), *La decisione robotica e il giudice amministrativo*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

L. Grimaldi (2022), *Costituzionalismo «post-umano» alla prova della decisione pubblica algoritmica*, in "federalismi.it", 2022, n. 34

T. Groppi (2020), *Alle frontiere dello Stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in "Consulta online", 28 settembre 2020

H. Kelsen (1960/1966), *La dottrina pura del diritto* (1960), trad. di M.G. Losano, Einaudi, 1966

M. Ladu, N. Maccabiani (2023), *L'individuo e la realtà digitale. Una questione costituzionale e democratica oltre la virtualità*, Editoriale Scientifica, 2023

M. Libertini, M.R. Maugeri, E. Vincenti (2021), *Intelligenza artificiale e giurisdizione ordinaria. Una ricognizione delle esperienze in corso*, in "Astrid Rassegna", 2021, n. 16

M. Luciani (2023), *Ogni cosa al suo posto*, Giuffrè, 2023

M. Luciani (2018), *La decisione giudiziale robotica*, in "Rivista AIC", 2018, n. 3, ora in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2018

M. Luciani (2016), *Interpretazione conforme a Costituzione*, in "Enciclopedia del diritto", Annali ix, 2016

V. Manes (2021), *Intelligenza artificiale e giustizia penale*, in U. Ruffolo (a cura di), "xxvi lezioni di diritto dell'intelligenza artificiale", Giappichelli, 2021

V. Manes (2020), L'*oracolo algoritmico e la giustizia penale*, in U. Ruffolo (a cura di), "Intelligenza artificiale - Il diritto, i diritti, l'etica", Giuffrè, 2020

A.A. Martino (2020), *Chi teme i giudici robot*, in "Rivista italiana di informatica e diritto", 2020, n. 2

D. Martire (2022), *Intelligenza artificiale e Stato costituzionale*, in "Diritto pubblico", 2022, n. 2

F. Modugno (2012), *Interpretazione giuridica*, Cedam, 2012

C. Napoli (2020), *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in "Rivista AIC", 2020, n. 3

A. Pace (2001), *Metodi interpretativi e costituzionalismo*, in "Quaderni costituzionali", 2001, n. 1

A. Pajno (2022), *L'uso dell'intelligenza artificiale nel processo tra problemi nuovi e questioni antiche*, in "Biolaw Journal", 2022, n. 1

L. Palmieri (2024), *Il deposito telematico tra esigenze efficientiste e garanzie difensive*, in "Diritto penale e processo", 2024, n. 4

A. Papa (2022), *Intelligenza Artificiale e decisioni pubbliche tra tecnica, politica e tutela dei diritti*, in "federalismi.it", 2022, n. 22

C. Pinelli (2019), *Certezza del diritto e compiti dei giuristi*, in "Diritto pubblico", 2019, n. 2

C. Pinelli (2016), *Il giudice e la legge*, in "Rivista AIC", 2016, n. 3

O. Pollicino (2023), *Il potere digitale*, in "Enciclopedia del diritto", v, Potere e costituzione, diretto da M. Cartabia e M. Ruotolo, Giuffrè, 2023

A. Punzi (2019), *Judge in the machine. E se fossero le machine a restituirci l'umanità del giudicare?*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

S. Quattrocolo (2019), *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in "Cassazione Penale", 2019, n. 4

S. Romano (1947/2013), *Frammenti di un dizionario giuridico* (1947), ora in Id., "L'ultimo' Santi Romano", Giuffrè, 2013

U. Ruffolo (2021), *La decisione robotica, la machina sapiens come "avvocato generale" ed il primato del giudice umano: una proposta virtuosa*, in Id. (a cura di), "xxvi lezioni di diritto dell'intelligenza artificiale", Giappichelli, 2021

U. Ruffolo (a cura di) (2021-a), *xxvi lezioni di diritto dell'intelligenza artificiale*, Giappichelli, 2021

A. Santosuosso, G. Sartor (2022), *La giustizia predittiva: una visione realistica*, in "Giurisprudenza italiana", 2022, n. 7

M. Sciacca (2023), *Algoritmo e giustizia alla ricerca di una mite predittività*, in "Persona e mercato", 2023, n. 1

A. Simoncini (2023), *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in "Rivista AIC", 2023, n. 2

A. Simoncini (2020), *Amministrazione digitale algoritmica. Il Quadro costituzionale*, in R. Cavallo Perin, D.-U. Galetta (a cura di), "Il diritto dell'Amministrazione pubblica digitale", Giappichelli, 2020

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà*, in "Biolaw Journal", 2019, n. 1

A. Sterpa (a cura di) (2024), *L'ordine giuridico dell'algoritmo*, Editoriale Scientifica, 2024

A. Triggiano (2013), *Il sogno di una giustizia predittiva tra Seicento e Ottocento*, in "Rivista italiana per le scienze giuridiche", 2013, n. 13

G. Tuzet (2020), *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in "MediaLaws", 2020, n. 1

G. Ubertis (2024), *Processo penale telematico, intelligenza artificiale e Costituzione*, in "Cassazione penale", 2024, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0204 • articolo sottoposto a peer review • pubblicato in anteprima il 5 feb. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Omar Caramaschi

Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?

Le sfide poste dall'avvento dell'intelligenza artificiale portano il giurista ad interrogarsi su quali categorie e strumenti giuridici possano essere adatti ad affrontarle, altresì con riguardo alle forme di regolazione, su tutte quelle europee, orientate ad un bilanciamento tra l'interesse economico relativo allo sviluppo di un mercato digitale europeo e quello di tutelare i valori democratici dell'ordinamento europeo e i diritti e le libertà fondamentali degli individui. Si tratta di un bilanciamento di natura costituzionale, dal quale emerge il tentativo di adattare la cornice costituzionale europea alla nuova realtà digitale. In questo senso la soluzione dovrebbe giungere dagli strumenti e dalle categorie del diritto costituzionale e del costituzionalismo: i cambiamenti determinati dall'emergere delle tecnologie legate all'intelligenza artificiale ricadono su principi e valori costituzionali fondamentali per lo Stato costituzionale contemporaneo tanto che sono gli stessi rischi derivanti dall'AI a sollecitare con forza il costituzionalismo a riscoprire il proprio ruolo di limitazione del potere e di garanzia dei diritti fondamentali.

Intelligenza artificiale – AI Act – Costituzionalismo – Costituzionalismo digitale

Constitutionalism in front of artificial intelligence: new challenges, what solutions?

The challenges determined by the advent of artificial intelligence lead the jurist to question which categories and legal instruments can be suitable to address them, also with regard to the forms of regulation, especially the European one, oriented to a balance between the economic interest relating to the development of a European digital market and that of protecting the democratic values of the European legal system and the fundamental rights and freedoms of individuals. This is a balance of a constitutional nature, from which emerges the attempt to adapt the European constitutional framework to the new digital reality. In this sense, the solution should come from the instruments and categories of constitutional law and constitutionalism: the changes determined by the appearance of technologies connected to artificial intelligence fall on fundamental constitutional principles and values for the contemporary constitutional State; therefore, the same risks deriving from AI forcefully urge constitutionalism to rediscover its role of limiting power and guaranteeing fundamental rights.

Artificial intelligence – AI Act – Constitutionalism – Digital constitutionalism

L'Autore è ricercatore (RTD-A) in Diritto costituzionale e pubblico presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Genova

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili sostanziali* a cura di Francesca Bailo e Michele Francaviglia

Questo lavoro è stato finanziato dal progetto NextGenerationEU "Security and Rights in CyberSpace" (SERICS) e dal progetto NextGenerationEU "Digitalization of the judiciary functions: trends, perspectives and risks" (PRIN 2022 PNRR, codice progetto: P2022PRBCS, CUP D53D23022420001). L'articolo costituisce una versione ampliata e rivista dei paper presentati al VII Congresso del Seminario italospagnolo (Napoli, 2-4 ottobre 2024) e alla V Conferenza italiana di ICON-S (Trento, 18-19 ottobre 2024)

Sommario: 1. Introduzione: Unione europea e costituzionalismo alla prova dell'intelligenza artificiale. – 2. Unione europea e intelligenza artificiale: la nuova stagione normativa europea in ambito tecnologico e l'*AI Act*. – 3. Dalla "rivoluzione digitale" al "costituzionalismo digitale"? – 4. Alcune osservazioni sulla "natura" e sul "futuro" del costituzionalismo digitale e cenni conclusivi.

1. Introduzione: Unione europea e costituzionalismo alla prova dell'intelligenza artificiale

Sempre più frequentemente l'Unione europea adotta – come conseguenza della comparsa della "società del rischio"[1] – un approccio basato sul rischio, dal diritto ambientale e dalla tutela della salute fino alla regolazione delle tecnologie digitali[2] con particolare riguardo all'intelligenza artificiale[3], in modo particolare al fine di accrescere la responsabilità degli attori pubblici e privati quanto agli effetti di queste tecnologie e alla tutela dei dati personali[4].

In questa direzione muovono il Regolamento generale sulla protezione dei dati o c.d. GDPR (*General Data Protection Regulation*, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), il Regolamento sui servizi digitali o c.d. DSA (*Digital Services Act*, Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2020 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE) e il più recente Regolamento sull'intelligenza artificiale o c.d. *AI Act*[5] (*Artificial Intelligence Act*, Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica

1. Cfr. Beck 1986; Lupton 2016.
2. Cfr. Longo 2024, spec. p. 72, secondo il quale «[n]el settore della salute, dell'ambiente e del welfare si trovano atti normativi che hanno come loro oggetto di regolazione il rischio. Come si è già fatto presente, a partire dalla metà degli anni '10, in concomitanza con l'espansione dell'economia dei dati, la regolazione del rischio digitale è divenuta una delle più importanti categorie usate dall'Unione per intervenire nel ricco mercato dei servizi e delle piattaforme digitali. Questa espansione ha portato i commentatori a sostenere che l'oggetto di tutta l'attività normativa in materia di digitale a livello europeo viene oggi definito o ridefinito nei termini della *risk regulation*» (sul punto v. Alemanno 2017).
3. Il tema dell'intelligenza artificiale è ormai al centro dell'interesse della dottrina giuridica; v., tra gli altri, Ruffolo 2020; Frosini 2020-a; Santosuosso 2020; Alpa 2021; Ruffolo 2021; Sartor 2022; Fazio 2023; Miniscalco 2024.
4. Cfr. Dunn–De Gregorio 2022-a; Longo 2024.
5. Tra i vari commenti in dottrina, specialmente prima dell'adozione definitiva nell'atto, v. Casonato–Marchetti 2021; La Vattiata 2021; Ebers 2022; Adinolfi 2022; Contissa–Galli–Godano–Sartor 2022; Martire 2022; Finocchiaro 2022-a; Novelli–Casolari–Rotolo et al. 2023; Almada–Petit 2023; Alaimo 2023; Schepisi 2023; Mancioppi 2024; Novelli 2024. Tra i commenti più recenti, successivi all'approvazione dell'*AI Act*, v. tra gli altri Lo Sapio 2022; Formisano 2024; Zaccaroni 2024; Cirone 2024; Inglese 2024; Alaimo 2024.

i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828).

Nonostante talune differenze, sembrerebbe potersi individuare, quale elemento qualificante, l'obiettivo comune di conseguire, specialmente in tema di intelligenza artificiale, un bilanciamento di interessi, in particolare tra l'interesse economico relativo allo sviluppo di un mercato digitale europeo aperto sul piano globale e quello, spesso contrapposto al primo, di tutelare i valori democratici dell'ordinamento europeo e i diritti e le libertà fondamentali degli individui. Si tratta di un bilanciamento di natura spiccatamente costituzionale, dal quale emerge il tentativo di adattare la cornice costituzionale europea alla nuova realtà digitale.

Muovendo in particolare verso le sfide poste dall'intelligenza artificiale, specialmente nella prospettiva del diritto costituzionale[6], emergono, nell'affermazione della c.d. società algoritmica[7], tutti i rischi che una simile tecnologia pone nei confronti delle garanzie giuridiche che dovrebbero tutelare e salvaguardare le persone dalle inopportune ingerenze di questa nuova forma di potere tecnologico[8].

In tale mutato contesto risulta opportuno interrogarsi su quali categorie e strumenti giuridici possano essere adatti al fine di affrontare le sfide poste dall'avvento dell'intelligenza artificiale, e la soluzione dovrebbe giungere, nuovamente, dai principi, dagli strumenti e dalle categorie del diritto costituzionale e del costituzionalismo contemporaneo. Ciò trova una spiegazione nel fatto che i cambiamenti determinati dall'emergere delle tecnologie legate all'intelligenza artificiale ricadono su principi e valori costituzionali fondamentali per lo Stato costituzionale contemporaneo – vedi su tutti il principio di uguaglianza o la privacy – tanto che sono gli stessi rischi derivanti dall'AI a sollecitare con forza il diritto costituzionale a riscoprire il proprio ruolo di limitazione del potere e di garanzia dei diritti fondamentali. Cosicché proprio le categorie del costituzionalismo contemporaneo potrebbero indirizzare sia i legislatori (tanto a livello nazionale che sovranazionale e perfino globale) sia i soggetti regolatori nel mettere a punto una disciplina normativa ovvero regolatoria dell'intelligenza artificiale che sia "umanocentrica" (v. *infra*), vale a dire capace di «valorizzare la centralità e il rispetto degli esseri umani quali obiettivi e valori centrali nell'uso di questa tecnologia»[9].

2. Unione europea e intelligenza artificiale: la nuova stagione normativa europea in ambito tecnologico e l'*AI Act*

Gli atti europei poc'anzi menzionati si inserirebbero nel solco di una "nuova stagione" normativa europea caratterizzata dalla volontà del legislatore europeo di riappropriarsi del ruolo di *law maker* che, in modo particolare nel settore digitale, è stato esercitato di fatto e per un periodo piuttosto lungo da parte della Corte di giustizia dell'Unione europea[10].

6. In dottrina v. sul punto Casonato 2019; Simoncini 2019; D'Aloia 2020; Colapietro–Moretti 2020, p. 359 ss. Nella dottrina spagnola v., tra gli altri, Sánchez Barrilao 2016; Balaguer Callejón 2023-a; Balaguer Callejón 2023-b.
7. V., *ex multis*, Bassini–Liguori–Pollicino 2018; Pajno–Bassini–De Gregorio et al. 2019; Fioriglio 2021; Micklitz–Pollicino–Reichman et al. 2021.
8. Cfr. Fasan 2022, spec. pp. 189-190. Sul punto v. anche Rodotà 2012, p. 402 ss.
9. Cfr. Fasan 2022, p. 190. Secondo l'A., inoltre, «[q]uesti elementi, dunque, attribuiscono al diritto costituzionale un ruolo chiave nell'individuare gli strumenti idonei ad affrontare i nuovi rischi posti dall'uso di una tecnologia come l'AI e nel garantire che gli stessi vengano arginati e mitigati da un impianto normativo e regolatorio volto ad assicurare il pieno rispetto dei diritti e delle libertà delle persone che si trovino ad interagire e ad utilizzare questi sistemi intelligenti. In tale contesto, alcuni tra i principi costituzionali riconosciuti e tutelati dagli ordinamenti giuridici contemporanei assumono una funzione di preminenza rispetto alla prospettiva regolatoria delineata, contribuendo ad individuare i potenziali correttivi da adottare nei confronti delle questioni più problematiche poste dall'AI». Sulla rilevanza delle categorie del diritto costituzionale con riguardo all'intelligenza artificiale v. tra gli altri Simoncini 2017; Casonato 2019; Casonato 2020; Pollicino–De Gregorio 2021.
10. Cfr. Pollicino 2023-a, spec. pp. 582-583.

Non bisogna infatti dimenticare la rilevanza della giurisprudenza dei giudici di Lussemburgo – avviata come risposta all'inerzia del legislatore europeo – nell'aver reso l'Unione europea «una fortezza in materia di dati personali»[11]. Basti pensare, in tal senso, anche solo ad alcune delle decisioni più rilevanti in ambito di tutela della privacy, come la nota sentenza *Google Spain*[12] alla quale si deve l'introduzione del c.d. diritto all'oblio – ovverosia il diritto di un individuo di richiedere ai gestori dei motori di ricerca e dei siti web di rimuovere, e quindi deindicizzare, informazioni e dati personali che lo riguardano al ricorrere di determinate condizioni – in seguito formalizzato nell'art. 17 del Regolamento generale sulla protezione dei dati del 2016. Oppure alle sentenze *Digital Rights Ireland*[13] o *Schrems*[14], attraverso le quali la Corte di giustizia ha manifestato una prima forte reazione all'emergere di nuove forme di potere digitale, nella misura in cui i giudici hanno cercato di ampliare notevolmente l'ambito di applicazione dei diritti previsti agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea – vale a dire il diritto al rispetto della vita personale e della vita familiare e il diritto alla protezione dei dati di carattere personale – non più limitandosi a tutelare gli individui nei confronti di eventuali ingerenze rispetto a tali diritti da parte del potere pubblico, bensì anche con specifico riguardo a quelle determinate dai nuovi poteri privati digitali (v. *infra*)[15].

Vi è stata quindi una stagione giurisprudenziale di intenso "attivismo" da parte della Corte di giustizia[16] – non priva di "controindicazioni" – la quale ha trovato la sua giustificazione nella riscontrata necessità di adeguare la normativa vigente al nuovo contesto tecnologico digitale, specialmente con l'obiettivo di promuovere e tutelare, anche nell'ambito della nuova società algoritmica, i valori fondamentali della democrazia costituzionale europea[17]. Ciononostante l'Unione europea ha cercato di ovviare al rischio di uno squilibrio nella separazione dei poteri, affrontando l'emergere della società algoritmica e dei nuovi poteri digitali non più soltanto attraverso l'importante versante giurisprudenziale, ma anche (e soprattutto) con il recupero della propria funzione legislativa e normativa – forte della legittimazione derivante dal circuito democratico-rappresentativo – così inaugurando una nuova stagione di costituzionalismo digitale (v. *infra*), ovverosia una fase di interventi normativi attraverso cui l'Unione europea ha inteso (e intende tuttora) regolare il fenomeno tecnologico-digitale attraverso gli strumenti peculiari del costituzionalismo europeo e contemporaneo proprio al fine di tutelarne e promuoverne i valori e i principi[18].

11. Dunn–Pollicino 2024, pp. 28-29.
12. CGUE, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, sentenza del 13 maggio 2014 (Grande Sezione).
13. CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri, e Kärntner Landesregierung e altri*, sentenza dell'8 aprile 2014 (Grande Sezione).
14. CGUE, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015 (Grande Sezione).
15. Cfr. Dunn–Pollicino 2024, spec. p. 29; sul punto v. anche Pollicino 2018, p. 264 ss.
16. La dottrina su tale giurisprudenza della Corte di giustizia è a dir poco abbondante. V. per tutti Finocchiaro 2015.
17. Cfr. Dunn–Pollicino 2024, spec. pp. 30-31. Gli AA. individuano in particolare tre controindicazioni nella stagione giurisprudenziale poc'anzi descritta: la prima riguarda l'accrescimento dello sbilanciamento nella separazione dei poteri tra il versante giudiziario e quello politico-legislativo; la seconda concerne la frammentazione che sarebbe derivata, a livello sovranazionale e specialmente nazionale, da un'eccessiva diversificazione nell'applicazione generale di regole di natura giurisprudenziale ideate per il singolo caso concreto; la terza, infine, attiene alla rimessione agli stessi attori privati gestori delle piattaforme di rilevanti scelte concernenti l'applicazione di quegli stessi diritti e valori che la Corte di giustizia ha cercato di rafforzare proprio per salvaguardarli dal potere privato digitale.
18. *Ibidem*.

Tale mutamento nell'approccio normativo dell'Unione europea si è verificato già a partire dal GDPR, il quale ha regolamentato e formalizzato molte delle posizioni negli anni espresse dalla Corte di Lussemburgo, di fatto traslando, come si è in parte già sostenuto, la protezione dei dati personali da una concezione prevalentemente orientata sul profilo economico a una invece racchiusa nella cornice costituzionale della Carta dei diritti fondamentali dell'Unione europea, in particolare degli artt. 7 e 8[19].

E in seguito tale cambio di propensione si è verificato anche con il *Digital Services Act* laddove vi è stato un deciso cambio di paradigma nella misura in cui il legislatore europeo è intervenuto nella limitazione dei poteri delle piattaforme online attraverso la previsione di garanzie di natura procedurale – che possono in qualche modo essere viste non solo come un tentativo di adeguare l'economia digitale ai principi e ai valori europei, ma anche come una reazione all'affermarsi di forme di potere privato (v. *infra*) – altresì predisponendo la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale[20], che individua un approccio "umanocentrico" come guida per la transizione digitale europea[21].

Da ultimo il recente *Artificial Intelligence Act* con il quale l'Unione europea affronta compiutamente, e per la prima volta con un regolamento, il tema dell'intelligenza artificiale[22], in particolare

19. Cfr. Pollicino 2023-a, pp. 583-584.

20. Cfr. Parlamento europeo, Consiglio e Commissione, *Dichiarazione comune sui diritti e i principi digitali per il decennio digitale* (2023/C 23/01), 23 gennaio 2023.

21. Cfr. De Gregorio 2023, spec. pp. 75-76. Secondo l'A. tale Dichiarazione «aims to put people at the center and foster solidarity and inclusion, freedom of choice, participation in the digital public space, safety, security and empowerment, and sustainability. It is an expression of the consolidation of digital constitutionalism, thus underlining how the digital future of the EU will likely be based on a digital compass guided by European (constitutional) values». Sul punto v. anche De Gregorio 2021-a.

22. Prima dell'*AI Act* vi sono stati diversi interventi normativi di *soft law*. Tra questi si pensi alla Risoluzione del Parlamento 2015/2103 (INL) del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, alla Comunicazione della Commissione europea su "L'intelligenza artificiale per l'Europa" COM(2018) 237 del 25 aprile 2018, alla Comunicazione della Commissione europea relativa al "Piano coordinato sull'intelligenza artificiale" COM(2018) 795 del 7 dicembre 2018, alla Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)), alla Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), alla Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale (2020/2266(INI)), al Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia COM(2020) 65 della Commissione europea del 19 febbraio 2020, accompagnato dalla "Relazione al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità" COM(2020) 64. Da segnalarsi, inoltre, nell'ambito del Consiglio d'Europa, due importarti iniziative. La prima è la Carta etica sull'uso dell'Intelligenza artificiale nei sistemi giudiziari adottata nel dicembre 2018 dall'European Commission for the Efficiency of Justice (CEPEJ). La seconda è la Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto (CM(2024)52), adottata all'unanimità dal Comitato dei Ministri del Consiglio d'Europa il 17 maggio 2024, la quale rappresenta il primo strumento internazionale pattizio avente come oggetto la regolazione dell'intelligenza artificiale nel rispetto della *rule of law* e dei diritti fondamentali. La Convenzione crea un quadro giuridico comune per garantire che le attività collegate all'intelligenza artificiale siano «fully consistent with human rights, democracy, and the rule of law» (art. 1), in piena sintonia con il diritto europeo e con l'*AI Act*. La Commissione ha firmato, per conto dell'Unione europea, la Convenzione quadro in occasione della conferenza informale dei Ministri della giustizia del Consiglio d'Europa (COE) del 5 settembre 2024, con ciò manifestando l'intenzione dell'Unione di diventare parte della Convenzione, alla quale dovrà fare seguito una proposta di decisione relativa alla conclusione della stessa da sottoporre a Consiglio e Parlamento europeo.

non soltanto con l'intenzione di favorire lo sviluppo delle tecnologie legate all'intelligenza artificiale nell'Unione europea e del relativo mercato interno[23], ma allo stesso tempo con l'obiettivo esplicito di proteggere i "valori europei"[24]; vale a dire che il legislatore europeo interviene al fine di evitare usi impropri di questa tecnologia – e i relativi strumenti che potrebbero determinare pratiche quali manipolazione, sfruttamento e controllo sociale – proprio perché ciò sarebbe in contraddizione con i «valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori»[25].

23. Cfr. Donati 2021-a, spec. p. 461. Secondo l'A. la scelta di un regolamento (e non di una direttiva) è da apprezzare in quanto «permetterà di ridurre "la frammentazione giuridica" e di facilitare "lo sviluppo di un mercato unico per sistemi di IA leciti, sicuri e affidabili"».

24. Cfr. De Gregorio 2023, pp. 76-77. L'A. sostiene inoltre che «[t]his duality of goals is precisely the characterization of the European approach at the intersection between digital humanism and digital capitalism». V. anche Floridi 2021.

25. Cfr. punto 28 dei considerando, *AI Act*. I riferimenti ai valori europei e ai diritti fondamentali sono piuttosto ricorrenti specialmente nella parte introduttiva del regolamento. Nel punto 1 dei considerando emerge la necessità di proteggere i diritti fondamentali, laddove si afferma che lo scopo del Regolamento «è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale […] garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("Carta"), compresi la democrazia, lo Stato di diritto». Nel punto 2 dei considerando si ribadisce che il «regolamento dovrebbe essere applicato conformemente ai valori dell'Unione sanciti dalla Carta agevolando la protezione delle persone fisiche, delle imprese, della democrazia e dello Stato di diritto». Anche al punto 8 viene rimarcata l'importanza dei diritti fondamentali, intesi in questa circostanza come interessi pubblici da proteggere nell'ambito del quadro giuridico dell'Unione sull'intelligenza artificiale («Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo […] la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto»). Il rispetto dei diritti fondamentali e il principio democratico vengono poi evocati in tema di alfabetizzazione in materia di intelligenza artificiale (punto 20 dei considerando, «Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA»). Seguono i considerando 28 (menzionato in apertura), 61 e 62, con riguardo ai sistemi di intelligenza artificiale ad alto rischio coinvolti sia nei processi democratici sia nell'amministrazione della giustizia. Infine il considerando 176 dove nuovamente viene evidenziata l'importanza di tutelare i diritti fondamentali: «Poiché l'obiettivo del presente regolamento, vale a dire migliorare il funzionamento del mercato interno e promuovere la diffusione di un'IA antropocentrica e affidabile, garantendo nel contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e promuovendo l'innovazione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata o degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'art. 5 TUE». Nel testo del regolamento, invece, il riferimento a valori, diritti e principio democratico emerge già in apertura, tanto che l'art. 1, par. 1, afferma che lo scopo del Regolamento «è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione».

Si tratta, nuovamente, di un orientamento "antropocentrico"[26], nella misura in cui il Regolamento si pone come intendimento quello di assicurare la "sorveglianza umana" e la tutela delle libertà e dei diritti fondamentali con riferimento ai potenziali pericoli che provengono dall'utilizzo di sistemi e tecnologie di intelligenza artificiale[27].

Nondimeno, sebbene l'*AI Act* rappresenti uno sviluppo significativo nell'approccio europeo alla regolamentazione dell'intelligenza artificiale, dal quale emerge l'impegno da parte del legislatore di stabilire le coordinate normative entro cui poter sviluppare le tecnologie di intelligenza artificiale in una maniera costituzionalmente e democraticamente ragionevole[28], tale Regolamento è stato oggetto di talune critiche.

Ad esempio, è stato notato come, a fronte di rilevanti previsioni come la valutazione d'impatto sui diritti fondamentali per i sistemi di intelligenza artificiale ad alto rischio (art. 27) e l'esercizio di diritti procedurali di fonte alle autorità di vigilanza del mercato istituite o designate dagli Stati membri (art. 70), permangano alcuni motivi di preoccupazione, in particolare con riguardo all'adeguatezza o meno dell'apparato procedurale previsto a favore degli individui per la tutela dei propri diritti fondamentali[29].

E sempre a tal proposito non si è mancato di notare come il regime giuridico introdotto dall'*AI Act* potrebbe risolversi in una "burocratizzazione" del mercato europeo legato all'intelligenza artificiale – si pensi al fatto che sono previsti numerosi obblighi di natura spesso formale e non sostanziale, ovvero al nuovo sistema di certificazione dei prodotti di intelligenza artificiale – senza che da ciò derivi necessariamente un rilevante e sostanziale beneficio quanto alla tutela effettiva dei diritti fondamentali[30].

26. Comunicazione della Commissione europea dell'8 aprile 2019 "Creare fiducia nell'intelligenza artificiale antropocentrica" COM(2019) 168.
27. Cfr. Donati 2021-a, pp. 462-463. Sempre l'A. osserva come si tratti di un obiettivo ambizioso, ma molto difficile da realizzare per due ragioni principali. La prima è legata «allo sviluppo della banda larga ed alla crescente diffusione dell'internet of things, cioè la connessione a Internet di oggetti fisici. Un numero sempre maggiore di oggetti che impiegano sistemi di intelligenza artificiale, dai cellulari agli impianti domestici, dagli strumenti medici ai sistemi per la sicurezza dei trasporti etc., inizieranno verosimilmente ad interagire tra di loro, con effetti potenzialmente imprevedibili. […] In definitiva, il collegamento di algoritmi che operano in maniera significativamente autonoma dalle istruzioni inizialmente ricevute dai programmatori, perché basati su sistemi di auto-apprendimento, potrebbe accrescere la loro autonomia. In casi del genere, il principio della supervisione umana e i meccanismi di verifica e sorveglianza ex ante previsti dal regolamento potrebbero rivelarsi non adeguati». La seconda ragione, invece, riguarda il profilo istituzionale, in quanto il successo (o meno) dell'*AI Act* «dipenderà dalle istituzioni chiamate ad applicarlo. Il regolamento prevede, infatti, la costituzione di organismi nazionali di certificazione, chiamati ad effettuare la valutazione della conformità dei sistemi di IA ad alto rischio rispetto ai requisiti previsti dal regolamento. Ciascuno Stato membro dovrà inoltre istituire appositi organismi (le autorità di notifica), chiamate a valutare e notificare le autorità di certificazione». Si prevede inoltre «che gli organismi nazionali di certificazione dovranno essere indipendenti dai fornitori di sistemi di intelligenza artificiale e dovranno essere "organizzati e gestiti in modo da salvaguardare l'indipendenza, l'obiettività e l'imparzialità delle loro attività". L'attuazione della disciplina relativa all'organizzazione ed al funzionamento degli organismi di notifica e degli organismi nazionali di certificazione spetterà agli Stati membri».
28. Cfr. Dunn–Pollicino 2024, pp. 66-67, laddove gli AA. portano come esempio «l'introduzione, con riferimento ai sistemi di IA ad alto rischio, dell'obbligo di condurre una valutazione d'impatto sui rischi che tali sistemi possano determinare in capo ai diritti fondamentali della persona prima della loro messa in uso».
29. Paolucci 2024-b.
30. Cfr. Finocchiaro 2024, pp. 122-123, laddove inoltre si osserva che, da un punto di vista sostanziale, alla domanda se l'*AI Act* «realizzi una risposta ai pericoli, dalla discriminazione alla faziosità, che sono alla base della sua stessa genesi e se tuteli adeguatamente i diritti e i valori europei, dalla dignità della persona alla protezione dei dati personali, cui costantemente si appella», si deve rispondere che ad oggi il Regolamento «al di là del suo valore strategico nel contesto geopolitico, che ne costituisce il fondamento, essenzialmente definisce una

Inoltre, come si è menzionato in apertura, l'*AI Act* presenta un *risk-based approach*[31] – già presente, seppure con sfumature diverse, nel GDPR e nel *Digital Services Act*[32] – con un significativo passaggio verso un modello *top-down*[33]. Sono previste quattro categorie di rischio con riguardo ai sistemi di intelligenza artificiale (rischio inaccettabile; rischio alto; rischio limitato; rischio minimo), ma l'individuazione delle categorie di rischio e degli eventuali meccanismi di mitigazione e di salvaguardia non è più affidata alla discrezionalità dei soggetti destinatari del Regolamento, bensì si baserebbe su un automatismo previsto dall'alto dalla Commissione europea[34], pur con qualche rilievo

cornice di natura amministrativa per l'immissione nel mercato dei prodotti di intelligenza artificiale. Il quadro generale dovrà peraltro essere completato dalle norme tecniche e dagli standard, che rivestiranno un'importanza fondamentale, e sarà continuamente aggiornato».

31. Cfr. da ultimo Longo 2024, spec. p. 72 ss.

32. Dunn–De Gregorio 2022-a osservano come il GDPR sarebbe caratterizzato dal principio di accountability che viene «declinato in pratica anche attraverso il ricorso a un sistema regolativo basato sul rischio, in base al quale titolare e responsabile del trattamento sono tenuti a predisporre le misure tecnico-organizzative necessarie ad assicurare che il GDPR stesso venga rispettato» e pertanto essi «dovranno operare una valutazione di impatto delle loro attività e, sulla base di tale valutazione, elaborare la strategia migliore per ridurre i rischi di violazione dei diritti individuali». La categoria del rischio sarebbe poi presente anche nel *Digital Services Act*, laddove questo «introdurrebbe una serie di obblighi a carico dei service provider volti a incentivare, da un lato, una riduzione di contenuti illeciti nell'ambiente digitale e, dall'altro lato, modalità più trasparenti e garantistiche delle attività di moderazione stessa. A differenza del GDPR, il DSA individua direttamente quattro livelli differenti di rischio, sulla base dei quali vengono assegnati obblighi e doveri differenti. Se nel GDPR vi è dunque una delegazione completa, secondo un modello *bottom-up*, dei doveri di valutazione e mitigazione, il DSA si discosta da tale sistema, individuando i criteri oggettivi di classificazione dei provider. Tuttavia, questo passaggio da una logica *bottom-up* a una logica *top-down* non è ancora completo: soprattutto nel caso delle piattaforme online di dimensioni molto grandi, infatti, un ampio margine di discrezionalità è comunque previsto per la mitigazione di rischi sistemici connessi alle loro attività». Sul punto v. anche Longo 2024; secondo l'A., p. 79 ss., nel caso del GDPR «si usano strumenti di gestione del rischio per determinare se si è conformi a un determinato quadro normativo», essendo richiesto alle organizzazioni una valutazione dei «livelli di rischio associati alle loro attività di trattamento dei dati al fine di proteggere la persona fisica e i suoi diritti», tanto da sostenersi in dottrina che un simile approccio sarebbe «parte di un modello di regolamentazione noto come "meta-regolamentazione", a sua volta parte di un framework che è noto come "regolamentazione basata sui principi"» (v. Gellert 2020). Sempre secondo Longo 2024, spec. p. 75 ss., il rischio può essere utilizzato anche come giustificazione per la regolazione, specialmente «da parte delle istituzioni politiche per determinare i confini dell'intervento legittimo» (v. il rimando a Black 2010); è questo il caso del DSA, dal momento che gli obiettivi del Regolamento vengono «affidati all'introduzione di una serie di obblighi e di doveri di diligenza per i prestatori di servizi digitali secondo una struttura a strati di tipo "piramidale" (rovesciata) basata sul livello di rischio implicito nell'attività dei prestatori di servizio». In questo senso, infatti, non si tratterebbe più soltanto «di valutare il rischio di un abuso delle piattaforme da parte di "attori malintenzionati" che se ne servono per commettere reati o diffondere disinformazione, ma anche di verificare il funzionamento previsto (il design) dei social media stessi. In questo senso, i "rischi sistemici" sono definiti secondo quattro aree, le quali sono individuate in maniera ampia, con riferimento agli effetti per i diritti fondamentali protetti dalla Carta dei diritti fondamentali dell'UE, i sistemi e i meccanismi democratici, la salute e il benessere delle persone».

33. Sul punto v. De Gregorio 2023, pp. 78-80; Dunn–De Gregorio 2022-a; Pollicino–De Gregorio–Bavetta–Paolucci 2021.

34. Cfr. Dunn–De Gregorio 2022-a i quali sostengono inoltre che la prospettiva dell'*AI Act* sarebbe «per certi versi opposta a quella del GDPR. Se nel GDPR la valutazione del rischio e la predisposizione di misure atte a tutelare i diritti individuali alla riservatezza e protezione dei dati erano attività delegate direttamente al titolare e al responsabile del trattamento dati, nel caso dell'AI Act la prospettiva è rovesciata: è il regolamento

critico, ad esempio, circa le modalità di concreta individuazione delle categorie dei sistemi di intelligenza artificiale ad alto rischio[35].

L'*AI Act* di fatto offre un approccio *top-down* nel quale sono gli attori pubblici a definire le norme in grado di conformare ai valori europei l'implementazione delle tecnologie connesse all'intelligenza artificiale, sebbene una tale categorizzazione dall'alto potrebbe non essere in grado di tenere sufficientemente conto delle dimensioni e delle capacità espresse dai soggetti privati da regolare attraverso lo stesso Regolamento[36].

Inoltre, non sono previsti rimedi legali diretti a proteggere tali valori, bensì vengono forniti appropriati "standard giuridici" per l'intelligenza artificiale in grado di definire e circostanziare quali di queste tecnologie siano effettivamente conformi ai valori europei, ovverosia si sostiene che «the expansion of the rule of law aims to reduce the consolidation of the rule of tech beyond Europe»[37], sulla base dell'assunto per il quale, avendo l'Unione europea già dimostrato la propria capacità di influenzare le dinamiche globali attraverso il c.d. effetto Bruxelles[38], ciò in particolare potrebbe di nuovo verificarsi per mezzo dell'estensione del proprio *regulatory soft power* a livello globale anche in ambito tecnologico[39].

La nuova stagione normativa e gli interventi regolatori europei appena esaminati delineano come l'Unione europea abbia consapevolmente scelto di porsi quale «centro di potere sovrano» nell'ambito del proprio mercato interno digitale, in tal senso imponendo una regolazione tale da ridurre gli spazi di autonomia autoregolativa dei poteri digitali[40] e altresì affermando la propria c.d. sovranità digitale[41], da intendere come facoltà del

stesso a operare tale attività. In effetti, se è vero che è presente, con riferimento ai sistemi di IA ad alto rischio, la previsione dell'obbligo di istituire, attuare, documentare e mantenere un sistema di gestione dei rischi, è altresì vero che nell'ecosistema del Regolamento tale norma sembra avere un carattere per lo più residuale».

35. Cfr. Finocchiaro 2024, pp. 120-121; Paolucci 2024-a.

36. Cfr. Finocchiaro 2024, pp. 121-122.

37. De Gregorio 2023, pp. 78-80.

38. Cfr. Bradford 2020. Secondo l'A., p. 18, «EU has become the global regulatory hegemon unmatched by its geopolitical rivals. [This] challenges the critics' view that portrays the EU as a powerless global actor, and shows how such a criticism focuses on a narrow and outdated vision of what power means today (…) promulgates regulations that influence which products are built and how business is conducted, not just in Europe but everywhere in the world. In this way, the EU wields significant, unique, and highly penetrating power to unilaterally transform global markets, be it through its ability to set the standards in competition policy, environmental protection, food safety, the protection of privacy, or the regulation of hate speech in social media».

39. Secondo Donati 2021-a, p. 462, l'Unione europea avrebbe il vantaggio della prima mossa, dal momento che dopo l'approvazione del Regolamento «le imprese extra-europee dovranno uniformarsi ad esso per riuscire a vendere i propri prodotti e servizi nel mercato europeo», in tal modo favorendo «quel fenomeno, conosciuto come "effetto Bruxelles", che indica la capacità dell'Unione europea di adottar discipline che finiscono poi per diventare standard accettati a livello globale». Secondo l'A. nei mercati digitali si potrebbe verificare un «adeguamento alla più rigida disciplina applicata in mercati di grandi dimensioni, come quello dell'Unione europea. Spesso infatti le imprese, soprattutto quelle che hanno una dimensione multinazionale, preferiscono adattare i servizi ed i prodotti offerti allo standard più rigoroso imposto dall'Unione europea, piuttosto che affrontare i problemi derivanti dalla necessità di osservare una pluralità di standard diversi. Questo fenomeno, che si è già verificato nell'ambito della protezione dei dati personali ed in molti altri campi, potrebbe ragionevolmente prodursi anche nel settore dell'intelligenza artificiale». Sul punto v. anche Donati 2021-b. In senso critico v. Pollicino 2023-b; Lo Sapio 2022, spec. p. 273 ss.

40. Cavani 2023, spec. p. 244.

41. In dottrina v. tra gli altri Zeno-Zencovich 2015; Couture–Toupin 2019; Pohle–Thiel 2020; Bertola 2022; Celeste 2021; Santaniello 2022; Tiberi 2022; Finocchiaro 2022-b; Mangiameli 2023; Alpini 2022. Secondo Longo 2024, spec. p. 71, «l'approccio alla regolazione delle tecnologie digitali basato sul governo del rispettivo rischio è divenuto il cuore della strategia adottata dall'Unione europea. Le istituzioni dell'UE

potere pubblico di controllare e regolamentare il digitale[42], sebbene il concetto stesso di "sovranità digitale europea" sia piuttosto dibattuto non solo perché spesso usato in luogo e con il significato di "potere", ma anche in ragione della sua natura di affermazione politica piuttosto che giuridica, proprio nella misura in cui si tratterebbe di un obiettivo di carattere politico che si intende raggiungere (come espresso dalla Presidente della Commissione europea nel 2020 o da numerosi documenti ufficiali europei di varia natura[43]) e non di una situazione giuridica di fatto[44].

Vi sarebbe pertanto un nesso molto significativo tra l'ambizione alla sovranità digitale da parte dell'Unione europea e la stessa identità costituzionale europea, laddove la prima risulta funzionale al consolidamento di quel costituzionalismo digitale europeo (v. *infra*) che emergerebbe dalla regolamentazione europea in tema, in modo che quest'ultimo possa disporre dei poteri

hanno indicato in questa scelta la via principale per riappropriarsi della propria sovranità digitale, in opposizione all'approccio libertario degli Stati Uniti e in netto contrasto con l'approccio autoritario della Cina. Si deve prima al presidente Claude Junker e poi al suo successore Ursula von der Leyen la creazione di un regime europeo della regolazione del rischio tecnologico come base per la costruzione di un nuovo mercato europeo digitale. In tali strategie emerge un nuovo stile istituzionale e politico europeo in cui il ruolo della Commissione diviene propriamente quello di regolatore delle tecnologie, con una corrispondente diminuzione delle altre competenze. L'approccio alla regolazione del rischio digitale intende inoltre completare l'idea dello "stato regolatore" europeo».

42. Per Floridi 2020, spec. pp. 370-371, sovranità digitale significa sostanzialmente controllo sul digitale: «digital sovereignty, that is, for the control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities), in short, for the control of the digital»; con "controllo" l'A. intende «the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence. In this sense, control comes in degrees and above all can be both pooled and transferred».

43. Cfr. Discorso sullo stato dell'Unione pronunciato dalla Presidente Von der Leyen nella sessione plenaria del Parlamento europeo del 16 settembre 2020 laddove si menziona la "sovranità digitale dell'Europa"; ovvero numerosi documenti dell'Unione europea come le Comunicazioni della Commissione europea per la transizione digitale del 19 febbraio 2020 ("Plasmare il futuro digitale dell'Europa" COM(2020)67, "Strategia europea per i dati" COM(2020)66 e "Libro bianco sull'Intelligenza artificiale" COM(2020)65), la "Nuova strategia industriale per l'Europa" della Commissione europea del 10 marzo 2020, le conclusioni del Consiglio dell'Unione europea "Plasmare il futuro digitale dell'Europa" del 9 giugno 2020, la Comunicazione della Commissione europea del 9 marzo 2021 "Bussola per il digitale 2030: il modello europeo per il decennio digitale" COM(2021) 118.

44. Cfr. Finocchiaro 2022-b, p. 811. Secondo Magnani 2023, spec. pp. 802-803, l'utilizzo del concetto di sovranità parrebbe essere una forzatura, in quanto potrebbe al massimo essere «un efficace espediente retorico per sottolineare il valore tutto politico di regolare un ambito materiale di cruciale valore strategico». La sovranità digitale, inoltre, «intende ristrutturare la categoria stessa della sovranità a partire dalla diffusione delle tecnologie elettroniche informatiche. La nuova realtà del potere vedrebbe ormai come nuovi soggetti istituzionali dominanti non più, o non più primariamente, le risalenti istituzioni pubbliche statuali dotate di una circoscritta potestà materiale e territoriale, bensì gli inediti attori che si muovono nella sfera sociale del digitale. Da questo nuovo potere sovrano digitale sorgerebbe quindi la necessità di trasfigurare anche i concetti più classici del costituzionalismo per renderli finalmente aderenti alla realtà. Questo ambizioso tentativo di rileggere in chiave contemporanea la sovranità incontra tuttavia una difficoltà generale: si rischia di restare prigionieri in una infinita corsa a inseguire la fattualità, obliando, nell'inseguimento adattivo ai processi politici e sociali, che proprio le istituzioni classiche della sovranità, gli stati sovrani, sono i primi artefici di queste innovazioni sociali, e che con scelte politiche diverse essi potrebbero determinare anche nuovi assetti dei poteri privati. Insomma, la sovranità digitale sembra indicare o troppo o troppo poco».

adeguati a garantire la tutela dei diritti fondamentali[45]. Alla rivendicazione da parte del legislatore europeo della leadership in materia di regolazione dell'intelligenza artificiale deve necessariamente accompagnarsi – se si vuole evitare un intervento meramente "gestionale" – uno sforzo affinché il potere pubblico rinvenga gli strumenti giuridici più opportuni per tutelare i valori europei e difendere i diritti individuali fondamentali[46].

Tornando conclusivamente sul fattore rischio, questo accomuna gli atti normativi europei poc'anzi brevemente affrontati anche per il fatto di tendere – proprio attraverso questo concetto – a realizzare lo stesso obiettivo, vale a dire un bilanciamento tra interessi diversi, da un lato quello di natura economica legato all'innovazione e allo sviluppo di tecnologie digitali in grado di competere a livello internazionale in virtù della creazione di un mercato interno digitale, dall'altro quello legato alla tutela dei diritti e delle libertà fondamentali nonché dei valori democratici[47]. Sicché il rischio sarebbe una sorta di "proxy" per questa attività di bilanciamento che assume una dimensione significativamente costituzionale, in buona sostanza quindi adottando «una prospettiva costituzionalmente orientata al rischio», quest'ultimo da intendersi non solo come modello normativo, ma, in special modo, come strumento in grado di offrire un sistema giuridico equilibrato e in grado di bilanciare – e quindi tutelare – in misura uguale i vari interessi[48].

In questo senso vi è chi ha individuato una «constitutionalization of the digital world» ovverosia un processo di creazione di norme e regole in grado di liberare il potenziale del sottosistema sociale digitale, al tempo stesso formalizzando meccanismi di limitazione e protezione in grado di delimitare la legittimità delle attività dei sistemi digitali al fine di preservare l'autonomia delle altre sfere sociali e i diritti fondamentali degli individui[49]. Sicché si è diffusa l'idea di un «digital constitutionalism framework for Ai»[50] – sulla base della teorizzazione del costituzionalismo digitale,

45. Cfr. Cavani 2023, spec. p. 244.

46. Cfr. Finocchiaro 2022-b, p. 827.

47. Cfr. Dunn–Pollicino 2024, pp. 62-63, secondo i quali «emerge dal testo legislativo il duplice obiettivo del legislatore euro-unitario di contemperare la finalità di migliorare il funzionamento del mercato interno e quella di promuovere la diffusione di un'IA "antropocentrica e affidabile", che sia in particolare rispettosa "della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente" [art. 1, par. 1]. Un duplice obiettivo, quindi, indice nuovamente di una matrice volta a uno sviluppo costituzionalmente sostenibile dell'IA».

48. Cfr. Dunn–De Gregorio 2022-a. Sul punto v. anche Dunn–De Gregorio 2022-b.

49. Cfr. Palladino 2023, spec. pp. 523-524. Come nota Circiumaru 2021, la Commissione europea «recognises an important challenge for EU fundamental rights, posed by a potent technology which is being quickly developed and starts taking active steps to address it, for example by banning AI systems which would pose unacceptable risks to fundamental rights. In doing so, the Commission wants to protect EU citizens not only from AI systems developed and deployed in the EU but all the systems that can negatively impact them, regardless of the place where they are deployed».

50. Secondo Palladino 2023, pp. 532-533, «fundamental rights are quite explicitly conceived as a mean to attain "trustworthy AI", thereby ensuring AI uptake across society. Indeed, "building trust around the development and use of AI" is a pillar of the European Commission strategy "Artificial intelligence for Europe" (EU Com 2018), to be achieved by ensuring "an appropriate ethical and legal framework based on the Union's values and in line with the Charter of Fundamental Rights of the EU", a concept further developed in the communication, titled not by chance, "Building trust in human-centric artificial intelligence" (EU Com 2019)». Inoltre, «a key point was the drafting of the "Ethics guidelines for trustworthy AI" [European Commission High Level Expert Group on AI] in which AI trustworthiness is related to the compliance with a series of principles (respect for human autonomy, prevention of harm, fairness, explicability) and requirements (human agency and oversight; robustness and safety, privacy, transparency, diversity, environmental and societal well-being, accountability) grounded in fundamental rights, to be implemented through a mix of technical and non-technical methods (for example explanation, testing and validation methods; quality of service indicators; standardization, certification)».

su cui ci concentreremo più approfonditamente nei successivi paragrafi – finalizzato non solo a fornire attraverso i diritti fondamentali uno "scudo" contro i pericoli derivanti dalla digitalizzazione, ma anche a preservare il carattere politico delle nostre società quali ordinamenti democratico-costituzionali, in modo particolare se si considera che i sistemi di intelligenza artificiale «increasingly shape our collective and individual environments, entitlements, access to, or exclusion from, opportunities, and resources»[51].

E proprio in questa direzione sembrerebbe muovere l'Unione europea attraverso un cambio di paradigma dal "liberalismo digitale" al "costituzionalismo digitale", quest'ultimo, come si vedrà a breve, orientato alla protezione dei diritti fondamentali e dei valori democratici attraverso la limitazione del potere privato digitale[52], proprio perché è lo stesso piano di sviluppo digitale europeo che deve essere guidato e interpretato da una lettura costituzionalistica della regolazione del mondo digitale, in modo che siano i valori europei a indirizzare quest'ultima verso una maggiore coerenza e uniformità della disciplina regolatoria digitale all'interno del complessivo quadro normativo europeo[53].

3. Dalla "rivoluzione digitale" al "costituzionalismo digitale"?

L'ascesa della c.d. era digitale o era dell'informazione ha dischiuso nuovi scenari per il costituzionalismo contemporaneo, in ragione del fatto che esso si trova a confrontarsi sia con un significativo incremento della frammentazione della sovranità e con la moltiplicazione dei "nuovi sovrani globali"[54], sia con un mutamento della sovranità stessa che assume caratteri di natura essenzialmente tecnica. In questo senso la potenza da "fondare" e "limitare" non è più tanto quella pubblica dello Stato, ma emerge un nuovo tipo di potenza che assume tanto la forma pubblica quanto quella privata[55], vale a dire «il paradigma tecnologico che si presenta come dominante, come fattore di liberazione della persona e di innovazione irresistibile, dunque, irrinunciabile»[56].

In particolare, l'esposizione dei diritti fondamentali degli utenti-individui alle continue e numerose minacce derivanti dalla Rete, in questo senso intesa come interamente estranea alla disciplina costituzionale e totalmente svincolata dai valori e dagli strumenti tipici dei moderni ordinamenti democratico-costituzionali[57], e l'accresciuta consistenza delle sfide poste dalla tecnologia digitale, specialmente laddove si tratti di poteri privati[58], costringono il giurista a rivedere le proprie categorie tradizionali per adattarle al nuovo contesto digitale; ciò, tuttavia, non deve inopportunamente determinare la tentazione di considerare come irrimediabilmente superate le basilari ed indispensabili coordinate ordinamentali di natura costituzionale[59], dal momento che i fondamentali

51. Cfr. Yeung–Howes–Pogrebna 2020, spec. p. 81.
52. Cfr. De Gregorio 2021-b, spec. p. 59. L'A., spec. pp. 67 e 70, prosegue sostenendo che «the rise of European digital constitutionalism represents the end of the liberal EU approach and a potential basis for promoting a democratic digital environment in the EU». In particolare, questa nuova fase «should not be seen merely as an imperialist extension of constitutional values outside the EU territory but as a reaction of European constitutionalism to the challenges to human dignity in an algorithmic society. In this scenario, the evolution of European digital constitutionalism would oppose techno-determinist solutions and contribute to promoting the European model as a sustainable constitutional environment for the development of artificial intelligence technologies in the global context».
53. Cavani 2023, spec. p. 244.
54. Per tutti, cfr. Luciani 1993; Luciani 1996, spec. p. 160 ss.; Azzariti 2013-a, spec. pp. 50-51.
55. Cfr. Cavani 2023, spec. p. 224.
56. Simoncini 2017, p. 20.
57. Cfr. Cavani 2023, p. 245.
58. Il tema è presente nella riflessione giuridica da diverso tempo, si pensi a Bianca 1977 e, ancora prima, in senso analogo Cesarini Sforza 1929/1963; tra gli studi costituzionalistici v. Barile 1953; Lombardi 1970; oppure v. il fascicolo monografico n. 3, 2021, della rivista *Diritto Pubblico*, interamente dedicato al tema dei poteri privati.
59. Cfr. Tarli Barbieri 2021, spec. pp. 946-947.

– ovverosia gli elementi essenziali e solitamente incontestati della scienza costituzionalistica[60] – non sono mutati nei loro presupposti logici bensì necessitano di essere sottoposti a valutazione critica, al fine di riaffermarne la necessaria validità alla luce del nuovo contesto.

In sostanza, pare doveroso riprendere e ribadire le "ragioni" del costituzionalismo moderno[61], non tanto per rimodellarne i presupposti, quanto piuttosto per muovere dalla consapevolezza di una mutazione delle circostanze fattuali[62] al fine di riscoprirne il "fondamento utopico", ovverosia la limitazione del "sovrano" e la garanzia dei diritti[63]. Si tratta fondamentalmente di continuare «la lotta all'arbitrio, la limitazione, il contenimento, la frammentazione del potere»[64], in modo particolare del nuovo potere privato che governa il mondo digitale[65] (si pensi alle c.d. *big tech* o anche efficacemente definite quali «compagnie del digitale»[66]), proprio perché se non si vuole rinunciare all'aspirazione del costituzionalismo moderno di limitare il "sovrano" – anche laddove questo si nasconda e diffonda il suo potere[67] – nessuna delle sue forme deve sfuggire al "contenimento" del costituzionalismo[68].

Come conseguenza di ciò si è iniziato da più parti a discorrere di "costituzionalismo digitale"[69], laddove l'aggettivo "digitale" implica, in un certo senso, una nuova collocazione temporale e materiale del costituzionalismo a seguito dell'avvento del web e di Internet sul finire del XX secolo[70]. In questo senso "digitale" determina una nuova riflessione circa i reciproci rapporti tra tecnologie digitali e costituzionalismo, sicché l'accostamento dei due termini in "costituzionalismo digitale" altro non sarebbe che un nuovo "settore", sia teorico che pratico, in grado di tenere insieme in maniera dialetticamente dinamica sia l'influenza esercitata dalle tecnologie digitali sul costituzionalismo (e sulla sua evoluzione), sia la reazione del diritto

60. Cfr. Azzariti 2013-a.

61. Sulle ragioni del costituzionalismo, v., *ex multis*, Rosenfeld 1994; Fioravanti 2008; Prisco 2015; Lanchester 2018; Frosini 2021.

62. Cfr. Bifulco 2014, spec. p. 27. In questo senso, secondo Lacchè 2016, spec. p. 26, una generale riconsiderazione del costituzionalismo moderno nello spazio giuridico globale dovrebbe necessariamente «prendere atto delle trasformazioni, di una *global governance* instabile e frammentata, di poteri economici e sociali diffusi, di circuiti costituzionali sovranazionali, di movimenti chiamati a riattualizzare le lotte per la costituzione democratica nei grandi spazi contemporanei».

63. Cfr. Azzariti 2013-b, spec. p. 188; Cavani 2023, p. 245.

64. Ferrara 2008, spec. p. 377.

65. Sui poteri privati digitali v. tra gli altri, almeno nella dottrina italiana, Betzu 2021; Betzu 2022-a; Betzu 2022-b; Ferrarese 2022; Cremona 2023; Pollicino 2023-c.

66. Violante 2022, spec. p. 148, laddove, in maniera suggestiva, si riadatta al contesto digitale e globale attuale l'esempio delle compagnie commerciali che tra il Seicento e l'Ottocento hanno esercitato funzioni paragonabili a quelle degli Stati (si pensi alla Compagnia inglese delle Indie Orientali o alla Compagnia inglese della Baia di Hudson), in quanto si trattava di soggetti – dotati di esercito e di sistemi di amministrazione della giustizia – che occupavano vastissimi territori per sfruttarne le risorse naturali. Oggi le «aziende del digitale esplicano una sovranità digitale in uno spazio nuovo colonizzato solo da loro. Le "compagnie del digitale" […] hanno un potere politico di fatto che nessuno ha mai avuto: creano opinioni, hanno una funzione regolatrice della vita dei privati e degli Stati, rendono servizi indispensabili e per questo condizionano la qualità dell'attività privata e pubblica». A differenza delle vecchie compagnie commerciali che occupavano un territorio preesistente, «le nuove creano il territorio che occupano. Siamo di fronte ad una espansione bulimica di poteri privati che servono funzioni diventate di pubblico interesse».

67. Cfr. Azzariti 2013-a, p. 56.

68. Cfr. Luciani 1996, p. 161.

69. V., *ex multis,* Padovani–Santaniello 2018; Celeste 2019; Pollicino 2021-b; Celeste 2022; De Gregorio 2022-a; De Gregorio 2022-b; ; Sánchez Barrilao 2023.

70. Sul punto cfr. Redeker–Gill–Gasser 2018.

costituzionale contro il potere pubblico e privato delle nuove tecnologie digitali[71]. E per ricollegarci a quanto sostenuto poc'anzi – circa un ritorno al compito storico del costituzionalismo – si tratterebbe di una modalità per riconsiderare come l'esercizio del potere debba essere limitato e legittimato anche nel mondo digitale[72].

Senza volersi addentrare nell'ampio dibattito dottrinario attorno alla costruzione teorica del costituzionalismo digitale, basti qui osservare che, pur in parte condividendosi talune delle preoccupazioni sollevate da chi sostiene con forza un «costituzionalismo senza aggettivi»[73], può risultare utile servirsi di tale espressione nel momento in cui si intenda collocare il costituzionalismo nella "nuova" dimensione digitale[74].

Il costituzionalismo digitale, pertanto, condividendo i valori e le categorie del costituzionalismo contemporaneo, non sarebbe un tentativo di introdurre un "nuovo" costituzionalismo, bensì uno sforzo concettuale di adeguarsi al nuovo contesto determinato dalla tecnologia digitale[75], riconsiderando e riadattando le categorie del costituzionalismo alla luce proprio di quei cambiamenti prodotti sulle vite degli individui e delle collettività dalla tecnologia nel contesto della "nuova civiltà digitale"[76].

Essenzialmente il costituzionalismo digitale altro non sarebbe che il costituzionalismo contemporaneo per come lo abbiamo classicamente conosciuto il quale si vedrebbe «impegnato in una fase di rinnovamento, non di stravolgimento» affinché possa trovarsi nelle condizioni più adeguate per rispondere efficacemente alle nuove sfide derivanti dall'emergere incisivo della dimensione tecnologico-digitale, in modo tale da essere in grado di rispondere alla «geometria variabile del potere» digitale (sempre più privato) con «la geometria altrettanto variabile del costituzionalismo»[77].

Difatti, da una prospettiva costituzionalistica, a seguito del sorgere di questo potere in ambito tecnologico e dei nuovi "sovrani" digitali, la sfida che si presenta non riguarda soltanto la capacità del potere pubblico di regolare e disciplinare il settore digitale, ma anche l'abilità del diritto costituzionale e del costituzionalismo[78] di saper contrastare il potere privato digitale nella sua dimensione sempre più globale e nei rischi che ne derivano per la tutela dei diritti fondamentali, e in questo modo del costituzionalismo europeo di farsi "digitale"[79].

71. Cfr. De Gregorio 2021-b, p. 58.
72. Cfr. Suzor 2018, p. 4. Secondo l'A., in questo senso, dato che il «core ideal of the rule of law is that the exercise of power is limited by rules» e il costituzionalismo «is the political project of defining these limits», il costituzionalismo digitale sarebbe «the work of articulating limits on the exercise of power in a networked society […] The key challenge of digital constitutionalism is to identify how values of good governance can be protected in the digital age».
73. Luciani 2022, spec. p. 497. Infatti, secondo l'A. la ragione di ciò sarebbe la «volontà di salvaguardare le categorie tradizionali del costituzionalismo», e così «la teorizzazione di un vero e proprio costituzionalismo digitale […] costituisce un azzardo, di dubbia utilità sul piano dell'inquadramento dommatico dei problemi […]. Le nostre categorie, dunque, restano intatte anche a fronte di sfide come quella dell'innovazione tecnologica o quella dell'apparente dissoluzione del territorio».
74. Cfr. Cavani 2023, spec. pp. 246-247.
75. Sul punto v. Celeste 2019, p. 76 ss.
76. Cfr. Frosini 2020-b, spec. p. 468.
77. Pollicino 2021-a.
78. Secondo Suzor 2019, p. 173, «digital constitutionalism requires us to develop new ways of limiting abuses of power in a complex system that includes many different governments, businesses, and civil society organizations». In senso analogo anche Padovani–Santaniello 2018, p. 295 ss., secondo i quali il costituzionalismo digitale consisterebbe nel predisporre limiti all'esercizio del potere in una società in rete.
79. Cfr. De Gregorio 2021-b, spec. p. 42. Sul punto v. Cheli 2021, spec. p. 956, il quale osserva come il costituzionalismo digitale «non potrà assumere le sue forme definitive altro che nello spazio sovranazionale utilizzando quel patrimonio delle "tradizioni costituzionali comuni" che la Carta dei diritti fondamentali dell'Unione ha già da tempo richiamato e che le giurisprudenze dei vari paesi dell'Unione stanno da tempo valorizzando. Una

4. Alcune osservazioni sulla "natura" e sul "futuro" del costituzionalismo digitale e cenni conclusivi

Le elaborazioni dottrinarie testé brevemente tratteggiate non sono esenti da valutazioni critiche[80]; per esempio, secondo alcuni si tratta di teorizzazioni che, immaginando di adeguare i valori costituzionali al nuovo contesto digitale, finirebbero talvolta anche inavvertitamente per trasferire e tradurre «concetti secolari e assiologicamente pregnanti tradendone lo spirito e, dunque, assecondandone un'interpretazione quanto meno parziale», oppure, in termini più generali, l'espressione costituzionalismo digitale verrebbe identificata come «abuso di denominazione», laddove si avrebbe a che fare con una formula assai imprecisa e indeterminata, che viene adottata in maniera superficiale e senza considerare adeguatamente le relative implicazioni indesiderate, come, ad esempio, una condotta di svilimento del ruolo delle Costituzioni statali[81].

Ora a fronte di tali critiche – in alcuni casi anche (almeno parzialmente) condivisibili – si deve osservare come la configurazione strutturale fondamentale del costituzionalismo digitale non sia esclusivamente legata all'emergere di nuovi *digital bill of rights*, proprio perché all'affacciarsi di nuovi diritti legati alla dimensione digitale è altresì apparso evidente come si prospettino nuove forme di potere digitale che pongono seri interrogativi per il costituzionalismo contemporaneo democratico. Ciò non deve determinare un totale affidamento alla "retorica" dei diritti fondamentali, in particolare nella creazione di nuovi diritti appositamente codificati in risposta al nuovo contesto tecnologico – si pensi alle numerose carte dei diritti online, come la "Dichiarazione dei diritti in Internet" formalizzata dalla Camera dei deputati italiana nel 2015, le quali essendo essenzialmente strumenti di *soft law* non vincolanti non hanno provocato nessun incremento significativo quanto ad una maggiore protezione dei diritti coinvolti[82] – ma deve, al contrario, condurci a riscoprire «la doppia anima del concetto di costituzione, quale *bill of rights* ma anche quale *frame of government*»[83]. In questa direzione quindi il costituzionalismo digitale non può limitarsi ad essere configurato soltanto come una sorta di declinazione del costituzionalismo globale ovvero come un ampliamento della "retorica dei diritti" – la quale non necessariamente si dimostra essere la soluzione adatta per una tutela più consistente degli stessi – bensì dovrebbe significare un'espansione della prospettiva di analisi che includa il costituzionalismo nelle sue diverse forme, vale a dire liberale, sociale e, finanche, globale[84].

Nondimeno risulta rilevante osservare come la risposta del costituzionalismo alle sfide poste dal nuovo contesto digitale non possa avere una configurazione di natura esclusivamente giurisdizionale[85]; se è in qualche modo indubbia la considerevole attività svolta dai giudici – non soltanto costituzionali ma a più livelli – come "avanguardia" nell'aver colto in anticipo, quindi ben prima dell'avverarsi

linea che […] negli anni più recenti è già emersa nelle normazioni europee varate o in corso di formazione in tema di disciplina dei dati e di regolamentazione dell'intelligenza artificiale e che si esprime con molta chiarezza attraverso l'enunciazione di principi diretti a garantire l'impiego di algoritmi trasparenti, affidabili e controllabili, idonei cioè a garantire un'intelligenza artificiale, come viene scritto nei documenti europei, "umanocentrica"». V. inoltre Balaguer Callejón 2023-c, spec. p. 185, secondo il quale «[l]a constitucionalización del algoritmo debe verse también, desde esta perspectiva, en sentido europeo, abriendo la posibilidad de una aplicación efectiva por parte de la Unión Europea de los principios y valores que se derivan del patrimonio constitucional europeo».

80. V., *ex multis,* Maroni 2020; Golia 2022; Costello 2023; Terzis 2024; Pagallo 2024.

81. Betzu 2022-b, pp. 64-65.

82. Cfr. Dunn–Pollicino 2024, pp. 218-219; sul punto v. anche Bassini–Pollicino 2015; Redeker–Gill–Gasser 2018.

83. Pollicino 2023-a, pp. 586-587.

84. *Ibidem*. Sul punto v. anche de Abreu Duarte–De Gregorio–Golia 2023.

85. Si veda almeno Pollicino 2021-b; sul ruolo dei giudici nelle teorie del costituzionalismo globale v. per tutti Caramaschi 2022, spec. p. 97 ss.

della nuova conformazione tecnologica, e cercato di porre rimedio alle possibili frizioni tra diritti fondamentali, ciò non può giustificare una posizione per così dire privilegiata del potere giurisdizionale, ma appare imprescindibile riequilibrare i rapporti tra quest'ultimo e il potere legislativo, il quale spesso si trova in una posizione marginale[86]. Pertanto sarebbe quantomai opportuno per il costituzionalismo digitale assumere una dimensione politica pienamente costituzionale «che non insegua la realtà, ma la orienti, rompendo le catene che legano le persone al "capitalismo della sorveglianza"»[87]. Questo sarebbe confacente non solo perché l'approccio giurisdizionale comporta evidenti rischi di frammentazione del contesto giuridico di riferimento, con specifica attenzione alle tensioni cui verrebbe sottoposto il principio di certezza del diritto, ma anche, e specialmente, con riguardo all'urgente necessità del legislatore di riappropriarsi del proprio ruolo – solo suppletivamente e provvisoriamente integrato dai giudici – anche in ragione della valorizzazione del circuito politico rappresentativo che ne è la base di legittimazione[88].

Ciò si è verificato nell'ambito della stagione normativa europea poc'anzi osservata, con particolare riguardo all'emergere degli ambiti algoritmico-digitali, laddove il legislatore si è mostrato del tutto intenzionato ad opporre ai nuovi poteri privati digitali non più una visione "liberistica", bensì "costituzionale" al fine appunto di congegnare forme di limitazione di tali poteri (altresì prevenendone gli abusi e gli eccessi) e di tutela dei diritti fondamentali in quella che è stata definita come "prima fase" della stagione del costituzionalismo digitale.

A questo primo momento, caratterizzato «da una forte impostazione assiologico-sostanziale di matrice legislativa» non priva di criticità[89], farebbe seguito una "seconda fase" – quella attuale e potenzialmente anche futura – in cui il costituzionalismo digitale assume una configurazione non solamente assiologico-sostanziale, ma anche di matrice «procedurale o procedimentale» e, al fine di evitare la frammentazione normativa cui si faceva riferimento, un campo di applicazione in qualche misura «"orizzontale", non incentrato su singoli settori, ma trasversale»[90].

86. Cfr. Pollicino 2023-a, p. 588.

87. Betzu 2022-b, pp. 64-65.

88. Cfr. Dunn–Pollicino 2024, p. 220.

89. *Ivi*, pp. 222-223. Secondo gli AA. vi sarebbero due principali inconvenienti. Il primo è il «rischio di innescare un processo di frammentazione interna in cui si applicano determinate regole, anche relative a differenti modelli di responsabilità per le grandi piattaforme digitali, a seconda della specifica disciplina rilevante, con un margine, peraltro, non indifferente di manovra per gli stati membri – visto anche l'assai significativo numero di clausole aperte contenute nei regolamenti rilevanti, spesso delle vere e proprie direttive mascherate (questa è una caratteristica comune tanto del GDPR come dell'AIA)». Il secondo, invece, sarebbe «causato dal rischio che, puntando esclusivamente su una cornice valoriale di natura regionale […] per disciplinare uno strumento, o meglio un ecosistema, come quello digitale, per definizione transnazionale, vi sia un effetto di isolamento radicale della fortezza europea cui mancherebbero i ponti levatoi di collegamento con gli altri poli regionali rilevanti. Il che, ovviamente, ha forti probabilità di tramutarsi nel rischio di un mancato enforcement delle regole europee e, più in generale, della amplificazione delle distanze con l'altra sponda dell'Oceano, che mette a rischio la solidità di quel ponte transatlantico il cui esercizio di manutenzione è invece, come si è detto, cruciale per un effettivo contenimento, da parte del costituzionalismo moderno, dell'ormai consolidato potere digitale di natura privata».

90. *Ivi*, pp. 222-223. Secondo gli AA. si tratterebbe di «una nuova declinazione o rimodulazione» del costituzionalismo digitale «che tenta di risolvere le problematiche, in termini di opacità e mancata trasparenza, che emergono frequentemente nei meccanismi algoritmici propri dei nuovi poteri, attraverso garanzie procedurali che offrano rimedio all'assenza di garanzie sostanziali comparabili a quelle proprie dei rapporti con attori pubblici». Allo stesso tempo non si deve confondere una maggiore attenzione alla "dimensione procedurale" con la «radicalizzazione di tale orientamento che rischierebbe di trasformare lo stato in quella che Forsthoff avrebbe chiamato "una macroamministrazione priva di capacità politica"», dal momento «che qualsiasi tentativo di proceduralizzazione disconnesso da una base valoriale di riferimento sia destinato a risolversi in uno sterile esercizio di "feticismo procedurale"». Sul punto v. anche Pollicino 2023-d; De Gregorio 2023.

In definitiva, si deve osservare come le prospettive aperte dal cambio di paradigma determinato dall'avvento delle nuove tecnologie – su tutte l'intelligenza artificiale – richiedano un cambio di paradigma anche di natura costituzionale, vale a dire che la protezione e la tutela dei beni e dei valori costituzionali dovrebbero precedere la produzione delle applicazioni tecnologiche e pertanto diventa necessario assimilare i valori costituzionalmente protetti già nel momento stesso della progettazione delle macchine, conseguentemente ideando un diritto costituzionale "ibrido", ovverosia un diritto costituzionale in grado di conoscere e quindi di esprimersi nello stesso linguaggio della tecnologia digitale[91].

Riferimenti bibliografici

A. Adinolfi (2022), *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. I, il Mulino, 2022

A.M. Alaimo (2024), *Il Regolamento sull'Intelligenza Artificiale. Un treno al traguardo con alcuni vagoni rimasti fermi*, in "federalismi.it", 2024, n. 25

A.M. Alaimo (2023), *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in "federalismi.it", 2023, n. 25

A. Alemanno (2017), *The Past, Present and Future of Risk Regulation*, in "European Journal of Risk Regulation", vol. 8, 2017, n. 1

M. Almada, N. Petit (2023), *The EU AI act: a medley of product safety and fundamental rights?*, Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59

G. Alpa (2021), *L'intelligenza artificiale. Il contesto giuridico*, Mucchi, 2021

A. Alpini (2022), *La sovranità digitale europea*, in "Rivista di scienze della comunicazione e di argomentazione giuridica", 2022, n. 2

G. Azzariti (2013-a), *Il costituzionalismo moderno può sopravvivere?*, Laterza, 2013

G. Azzariti (2013-b), *La costituzione come norma e la crisi del costituzionalismo contemporaneo*, in "Rivista italiana per le scienze giuridiche", 2013, n. 4

F. Balaguer Callejón (2023-a), *Inteligencia artificial y cultura constitucional*, in F. Balaguer Callejón, I.W. Sarlet, C.L. Strapazzon et al., "Derechos fundamentales y democracia en el constitucionalismo digital", Aranzadi, 2023

91. Cfr. Simoncini–Suweis 2019, spec. p. 103. Sul punto v. anche Simoncini 2023, spec. pp. 38-39, il quale conclusivamente osserva che nella "nuova era" dell'integrazione tra uomini e macchine intelligenti, in particolar modo quando entrano in gioco le libertà costituzionali, il tema del linguaggio diviene dirimente; in questo scenario, «il diritto costituzionale, se vuole mantenere il suo statuto di argine e limite giuridico nei confronti di qualsiasi forma di potere sia politico che sociale, deve evitare che si vengano a creare "zone franche", in cui l'incomprensibilità di certi sistemi di IA renda di fatto non giustiziabili le decisioni prese sulla base di questi sistemi. Se da un lato, infatti, è del tutto impercorribile, ed invero non auspicabile, la strada di una reazione "neo-luddista" o anti-tecnologica, che voglia impedire lo sviluppo di questi risultati decisivi per il progresso della nostra civiltà, dall'altro questo stesso progresso deve mantenere centrale il valore della persona e delle sue relazioni, valore sul quale è fondato il nostro sistema costituzionale sia nazionale che europeo. In questa prospettiva, il tema del linguaggio impiegato dalle tecnologie "sociali" e della sua comprensibilità, diviene uno snodo centrale nel dibattito che sta accompagnando la trasformazione del diritto costituzionale nella nostra età tecnologica».

F. Balaguer Callejón (2023-b), *La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital*, in F. Balaguer Callejón, L. Cotino Hueso (coord.), "Derecho público de la inteligencia artificial", Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, 2023

F. Balaguer Callejón (2023-c), *La constitución del algoritmo*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, 2023

P. Barile (1953), *Il soggetto privato nella Costituzione*, Cedam, 1953

M. Bassini, L. Liguori, O. Pollicino (2018), *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

M. Bassini, O. Pollicino (a cura di) (2015), *Verso un Internet Bill of Rights*, Aracne, 2015

U. Beck (1986), *Risikogesellschaft. Auf dem Weg in eine andere Moderne,* Suhrkamp Verlag AG, 1986 (trad. it., *La società del rischio. Verso una seconda modernità*, Carocci, 2000)

V. Bertola (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", 2022, n. 1

M. Betzu (2022-a), *I baroni del digitale*, Editoriale Scientifica, 2022

M. Betzu (2022-b), *Poteri pubblici e poteri privati nel mondo digitale*, in P. Costanzo, P. Magarò, L. Trucco (a cura di), "Il diritto costituzionale e le sfide dell'innovazione tecnologica", Atti del Convegno Annuale dell'Associazione Gruppo di Pisa (Genova, 18-19 giugno 2021), Editoriale Scientifica, 2022

M. Betzu (2021), *I poteri privati nella società digitale: oligopoli e antitrust*, in "Diritto Pubblico", 2021, n. 3

C.M. Bianca (1977), *Le autorità private*, Jovene, 1977

R. Bifulco (2014), *La c.d. costituzionalizzazione del diritto internazionale: un esame del dibattito*, in "Rivista AIC", 2014, n. 4

J. Black (2010), *The Role of Risk in Regulatory Processes*, in R. Baldwin, M. Cave, M. Lodge (eds.), "The Oxford Handbook of Regulation", Oxford University Press, 2010

A. Bradford (2020), *The Brussel Effect. How the European Union Rules the World*, Oxford University Press, 2020

O. Caramaschi (2022), *Il costituzionalismo globale: teorie e prospettive*, Giappichelli, 2022

C. Casonato (2020), *Per un'intelligenza artificiale costituzionalmente orientata*, in A. D'Aloia (a cura di), "Intelligenza artificiale e diritto. Come regolare un mondo nuovo", FrancoAngeli, 2020

C. Casonato (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in "Diritto pubblico comparato ed europeo", 2019, fasc. speciale

C. Casonato, B. Marchetti (2021), *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3

V. Cavani (2023), *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in "Diritto pubblico comparato ed europeo", 2023, n. 1

E. Celeste (2022), *Digital Constitutionalism. The Role of Internet Bills of Rights*, Routledge, 2022

E. Celeste (2021), *Digital sovereignty in the EU: challenges and future perspectives*, in F. Fabbrini, E. Celeste, J. Quinn (eds.), "Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty", Hart, 2021

E. Celeste (2019), *Digital Constitutionalism: A New Systematic Theorisation*, in "International Review of Law, Computers & Technology", 2019, n. 1

W. Cesarini Sforza (1929/1963), *Il diritto dei privati* (1929), Giuffrè, 1963

E. Cheli (2021), *Conclusioni*, in "Osservatorio sulle fonti", 2021, n. 2

A. Circiumaru (2021), *EU Digital Constitutionalism, Digital Sovereignty and the Artificial Intelligence Act – A network perspective*, in "European Law Blog", 23 dicembre 2021

E. Cirone (2024), *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in "Quaderni AISDUE", 2024, fasc. speciale n. 2

C. Colapietro, A. Moretti (2020), *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in "BioLaw Journal - Rivista di BioDiritto", 2020, n. 3

G. Contissa, F. Galli, F. Godano, G. Sartor (2022), *La nuova Proposta di Regolamento europeo sull'Intelligenza artificiale: questioni giuridiche e approcci regolatori*, in R. Brighi (a cura di), "Nuove questioni di informatica forense", Aracne, 2022

R.Á. Costello (2023), Faux Ami*? Interrogating the normative coherence of 'digital constitutionalism'*, in "Global Constitutionalism", vol. 12, 2023, n. 2

S. Couture, S. Toupin (2019), *What does the notion of "sovereignty" mean when referring to the digital?*, in "New Media & Society", vol. 21, 2019, n. 10

E. Cremona (2023), *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Edizioni Scientifiche Italiane, 2023

A. D'Aloia (a cura di) (2020), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, FrancoAngeli, 2020

F. de Abreu Duarte, G. De Gregorio, A. Golia (2023), *Perspectives on Digital Constitutionalism*, in B. Brozek, O. Kanevskaia, P. Palka (eds.), "Research Handbook on Law and Technology", Edward Elgar Publishing, 2023

G. De Gregorio (2023), *The Normative Power of Artificial Intelligence*, in "Indiana Journal of Global Legal Studies", vol. 30, 2023, n. 2

G. De Gregorio (2022-a), *Digital Constitutionalism across the Atlantic*, in "Global Constitutionalism", vol. 11, 2022, n. 2

G. De Gregorio (2022-b), *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022

G. De Gregorio (2021-a), *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in "Diritti Comparati", 17 maggio 2021

G. De Gregorio (2021-b), *The rise of digital constitutionalism in the European Union*, in "International Journal of Constitutional Law", vol. 19, 2021, n. 1

F. Donati (2021-a), *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in "Il Diritto dell'Unione Europea", 2021, n. 3-4

F. Donati (2021-b), *Verso una nuova regolazione delle piattaforme digitali*, in "Rivista della Regolazione dei Mercati", 2021, n. 2

P. Dunn, G. De Gregorio (2022-a), *AI Act, rischio e costituzionalismo digitale*, in "Media Laws. Law and Policy of the Media in a Comparative Perspective", 22 aprile 2022

P. Dunn, G. De Gregorio (2022-b), *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in "Common Market Law Review", 2022, n. 2

P. Dunn, O. Pollicino (2024), *Intelligenza artificiale e democrazia*, Bocconi University Press, 2024

M. Ebers (2022), *Standardizing AI. The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. Di Matteo, M. Cannarsa, C. Poncibò (eds.), "The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics", Cambridge University Press, 2022

M. Fasan (2022), *I principi costituzionali nella disciplina dell'Intelligenza Artificiale. Nuove prospettive interpretative*, in "DPCE Online", 2022, n. 1

E. Fazio (2023), *Intelligenza artificiale e diritti della persona*, Edizioni Scientifiche Italiane, 2023

G. Ferrara (2008), *Conclusioni*, in M. Ruotolo (a cura di), "La Costituzione ha 60 anni. La qualità della vita sessant'anni dopo", Editoriale Scientifica, 2008

M.R. Ferrarese (2022), *Poteri nuovi. Privati, penetranti, opachi*, il Mulino, 2022

G. Finocchiaro (2024), *Intelligenza artificiale. Quali regole?*, il Mulino, 2024

G. Finocchiaro (2022-a), *La proposta di Regolamento sull'Intelligenza Artificiale: il modello europeo basato sulla gestione del rischio*, in "Il diritto dell'informazione e dell'informatica", 2022, n. 2

G. Finocchiaro (2022-b), *La sovranità digitale*, in "Diritto pubblico", 2022, n. 3

G. Finocchiaro (2015), *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. Resta, V. Zeno-Zencovich (a cura di), "Il diritto all'oblio dopo la sentenza Google Spain", RomaTre-Press, 2015

M. Fioravanti (2008), *Costituzionalismo*, Laterza, 2008

G. Fioriglio (2021), *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici*, in "Ars Interpretandi", 2021, n. 1

L. Floridi (2021), *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in "Philosophy & Technology", vol. 34, 2021, n. 2

L. Floridi (2020), *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in "Philosophy & Technology", vol. 33, 2020, n. 3

A. Formisano (2024), *L'impatto dell'intelligenza artificiale in ambito giudiziario sui diritti fondamentali*, in "federalismi.it", 2024, n. 22

T.E. Frosini (2021), *La lotta per i diritti. Le ragioni del costituzionalismo*, Editoriale Scientifica, 2021

T.E. Frosini (2020-a), *Liberté, Égalité, Internet*, Editoriale Scientifica, 2020

T.E. Frosini (2020-b), *Il costituzionalismo nella società tecnologica*, in "Il diritto dell'informazione e dell'informatica", 2020, n. 3

R. Gellert (2020), *The risk-based approach to data protection*, Oxford University Press, 2020

A. Golia (2022), *The Critique of Digital Constitutionalism*, Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2022-13, 2022

M. Inglese (2024), *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno*, in "Quaderni AISDUE", 2024, fasc. speciale n. 2

F.C. La Vattiata (2021), *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in "Diritto penale e Uomo", 2021, n. 6

L. Lacchè (2016), *Ripensare il costituzionalismo tra storia e mondo globale: realtà e sfide*, in "Giornale di storia costituzionale", 2016, n. 2

F. Lanchester (2018), *Il profumo del costituzionalismo*, in "Nomos", 2018, n. 2

G. Lo Sapio (2022), *Intelligenza artificiale: rischi, modelli regolatori, metafore*, in "federalismi.it", 2022, n. 27

G. Lombardi (1970), *Potere privato e diritti fondamentali*, Giappichelli, 1970

E. Longo (2024), *La disciplina del "rischio digitale"*, in F. Pizzetti (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024

M. Luciani (2022), *Relazione conclusiva*, in P. Costanzo, P. Magarò, L. Trucco (a cura di), "Il diritto costituzionale e le sfide dell'innovazione tecnologica", Atti del Convegno Annuale dell'Associazione Gruppo di Pisa (Genova, 18-19 giugno 2021), Editoriale Scientifica, 2022

M. Luciani (1996), *L'antisovrano e la crisi delle costituzioni*, in "Rivista di Diritto Costituzionale", 1996, n. 1

M. Luciani (1993), *Tramonto della sovranità e diritti fondamentali*, in "Critica marxista", 1993, n. 5

D. Lupton (2016), *Digital risk society*, in A. Burgess, A. Alemanno, J. Zinn (eds.), "Routledge Handbook of Risk Studies", Routledge, 2016

C. Magnani (2023), *Nuovi media, libertà di espressione e costituzionalismo*, in "Dirittifondamentali.it", 2023, n. 2

F.M. Mancioppi (2024), *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in "federalismi.it", 2024, n. 7

S. Mangiameli (2023), *La sovranità digitale*, in "Dirittifondamentali.it", 2023, n. 3

M. Maroni (2020), *Lawless: The Secret Rules That Govern Our Digital Lives - Book Review*, in "European Journal of Risk Regulation", 2020, n. 1

D. Martire (2022), *Intelligenza artificiale e Stato costituzionale*, in "Diritto pubblico", 2022, n. 2

H.-W. Micklitz, O. Pollicino, A. Reichman et al. (eds.) (2021), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021

N. Miniscalco (2024), *L'intelligenza artificiale in movimento. Impatto sui diritti costituzionali*, Cedam, 2024

C. Novelli (2024), *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in "federalismi.it", 2024, n. 2

C. Novelli, F. Casolari, A. Rotolo et al. (2023), *Taking AI risks seriously: a new assessment model for the AI Act*, in "AI & Society", 2023, n. 3

C. Padovani, M. Santaniello (2018), *Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system*, in "International Communication Gazette", vol. 80, 2018, n. 4

U. Pagallo (2024), *Dismantling Four Myths in AI & EU Law Through Legal Information 'About' Reality*, in H. Sousa Antunes, P.M. Freitas, A.L. Oliveira et al. (eds.), "Multidisciplinary Perspectives on Artificial Intelligence and the Law", Springer, 2024

A. Pajno, M. Bassini, G. De Gregorio et al. (2019), *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in "BioLaw Journal - Rivista di BioDiritto", 2019, n. 3

N. Palladino (2023), *A digital constitutionalism framework for Ai: security and fundamental rights in the Ai Act*, in "Rivista di Digital Politics", 2023, n. 3

F. Paolucci (2024-a), *Whatever it takes? The Al Act regulatory crucible*, in "Diritti Comparati", 22 gennaio 2024

F. Paolucci (2024-b), *Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights*, in "VerfBlog", 14 March 2024

F. Pizzetti (a cura di) (2024), *La regolazione europea della società digitale*, Giappichelli, 2024

J. Pohle, T. Thiel (2020), *Digital sovereignty*, in "Internet Policy Review", vol. 9, 2020, n. 4

O. Pollicino (2023-a), *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in "Quaderni costituzionali", 2023, n. 3

O. Pollicino (2023-b), *Washington effect o Bruxelles effect? Regolamentazioni dell'IA a confronto*, in "formiche", 31 ottobre 2023

O. Pollicino (2023-c), *Potere digitale*, in M. Cartabia, M. Ruotolo (a cura di), "Potere e Costituzione", Enciclopedia del Diritto, vol. 5, Giuffrè, 2023

O. Pollicino (2023-d), *The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism*, in "European Law Journal", vol. 29, 2023, n. 1-2

O. Pollicino (2021-a), *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali le sfide per il giurista (teorico e pratico)?*, in "Giustizia insieme", 15 aprile 2021

O. Pollicino (2021-b), *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Hart, 2021

O. Pollicino (2018), *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in V. Piccone, O. Pollicino (a cura di), "La Carta dei Diritti Fondamentali dell'Unione Europea. Efficacia ed effettività", Editoriale Scientifica, 2018

O. Pollicino, G. De Gregorio (2021), *Constitutional Law in the Algorithmic Society*, in H.-W. Micklitz, O. Pollicino, A. Reichman et al. (eds.), "Constitutional Challenges in the Algorithmic Society", Cambridge University Press, 2021

O. Pollicino, G. De Gregorio, F. Bavetta, F. Paolucci (2021), *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, in "Agenda digitale", 21 maggio 2021

S. Prisco (2015), *Costituzionalismi antichi e moderni tra strutture invarianti e specificità storiche*, in Aa. Vv., "Scritti in onore di Antonio D'Atena", Giuffrè, 2015

D. Redeker, L. Gill, U. Gasser (2018), *Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights*, in "International Communication Gazette", vol. 80, 2018, n. 4

S. Rodotà (2012), *Il diritto di avere diritti*, Laterza, 2012

M. Rosenfeld (1994), *Modern Constitutionalism as Interplay between Difference and Identity*, in Id. (ed.), "Constitutionalism, Identity, Difference, and Legitimacy: Theoretical Perspectives", Duke University Press, 1994

U. Ruffolo (a cura di) (2021), *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, 2021

U. Ruffolo (a cura di) (2020), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020

J.F. Sánchez Barrilao (2023), *Constitucionalismo digital: entre realidad digital, prospectiva tecnológica y mera distopía constitucional*, in F. Balaguer Callejón, I.W. Sarlet, C.L. Strapazzon et al., "Derechos fundamentales y democracia en el constitucionalismo digital", Aranzadi, 2023

J.F. Sánchez Barrilao (2016), *El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional*, in "Estudios De Deusto", 2016, n. 2

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Santosuosso (2020), *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, 2020

G. Sartor (2022), *L'intelligenza artificiale e il diritto*, Giappichelli, 2022

C. Schepisi (2023), *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. Falce (a cura di), "Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato", Giappichelli, 2023

A. Simoncini (2023), *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in "Rivista AIC", 2023, n. 2

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal - Rivista di BioDiritto", 2019, n. 1

A. Simoncini (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), "Diritti e libertà in Internet", Le Monnier, 2017

A. Simoncini, S. Suweis (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1

N. Suzor (2019), *Lawless: The Secret Rules That Govern Our Digital Lives*, Cambridge University Press, 2019

N. Suzor (2018), *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, in "Social Media + Society", 2018, n. 3

G. Tarli Barbieri (2021), *Considerazioni di sintesi sul ruolo delle autorità amministrative indipendenti nella regolazione delle decisioni algoritmiche*, in "Osservatorio sulle fonti", 2021, n. 2

P. Terzis (2024), *Against Digital Constitutionalism*, in "European Law Open", 25 July 2024

G. Tiberi (2022), *L'irresistibile ascesa della sovranità digitale europea*, in G. Ferri (a cura di), "Diritto costituzionale e nuove tecnologie", Edizioni Scientifiche Italiane, 2022

L. Violante (2022), *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in "BioLaw Journal - Rivista di BioDiritto", 2022, n. 1

K. Yeung, A. Howes, G. Pogrebna (2020), *AI Governance by Human Rights–Centered Design, Deliberation, and Oversight: An End to Ethics Washing*, in F. Pasquale, S. Das (eds.), "The Oxford Handbook of Ethics of AI", Oxford University Press, 2020

G. Zaccaroni (2024), *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in "Quaderni AISDUE", 2024, fasc. speciale n. 2

V. Zeno-Zencovich (2015), *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 4-5

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0231 • articolo sottoposto a peer review • pubblicato in anteprima il 1 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Alessandro Malacarne

Brevi osservazioni sulla c.d. "confessione intercettata": un dibattito ancora attuale tra spontaneità e consapevolezza

Il contributo esamina il rapporto tra la garanzia del diritto a non autoincriminarsi e l'istituto delle intercettazioni telefoniche, mettendo in luce le diverse impostazioni che emergono, nel panorama italiano, dal dibattito dottrinale e giurisprudenziale.

Confessione – Nemo tenetur se detegere – Intercettazioni telefoniche e telematiche

Observations on the so-called "intercepted confession": a still relevant debate between spontaneity and awareness

The paper focuses on the relationship between the *nemo tenetur se detegere* and telephone tapping, highlighting the different approaches that have emerged from literature and jurisprudential debates in Italy.

Confession – Nemo tenetur se detegere – Wiretapping

L'Autore è assegnista di ricerca in Diritto processuale penale presso il Dipartimento di giurisprudenza dell'Università di Genova

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili sostanziali* a cura di Francesca Bailo e Michele Francaviglia

Sommario: 1. Introduzione e inquadramento del problema. – 2. Fondamento e portata applicativa del diritto al silenzio nelle intercettazioni. – 2.1. La tesi della spontaneità. – 2.2. La tesi della consapevolezza: critiche. – 3. Conseguenze processuali dell'utilizzabilità della c.d. confessione intercettata. – 4. Sintesi.

1. Introduzione e inquadramento del problema

Nonostante le origini risalenti, il diritto al silenzio e alla protezione contro l'autoincriminazione[1] conserva ancora oggi viva attualità, alimentando questioni irrisolte sia a livello teorico che nella prassi giudiziaria[2]. Un tanto si deve, in particolare, all'evoluzione tecnologica e alla pervasiva digitalizzazione che caratterizza ormai ogni istante di vita quotidiana: tali fenomeni, a ben vedere, hanno conferito a siffatto "strumento di difesa" nuova linfa vitale, rendendolo un presidio essenziale a tutela della persona – nella sua duplice dimensione: corporea e immateriale[3] – contro le crescenti ingerenze realizzate dal potere pubblico nel corso del procedimento penale.

Più precisamente, il progressivo ampliamento degli strumenti investigativi (anche di natura informatica) a disposizione dell'autorità inquirente e l'impiego – in costante crescita – di apparecchi di archiviazione massiva di *bit*, ha determinato un significativo mutamento dell'equilibrio tra esigenze di accertamento e diritti fondamentali, rendendo possibile l'apprensione di dati e di materiale conoscitivo non solo dall'ambiente esterno, ma anche dal corpo e dalla mente della persona sottoposta a indagine. A titolo esemplificativo, si consideri l'impiego di metodi e tecniche volti a ottenere informazioni biometriche necessarie onde accedere a dispositivi (smartphone, computer, tablet, etc.) protetti da sistemi di riconoscimento personale[4] – come impronte digitali, facciali o vocali –, oppure a inoculare *malware* nei terminali in uso al prevenuto, al fine di compromettere l'*host* ed ottenerne il controllo remoto[5]. Si pensi, ancora, all'ipotesi in cui gli organi del procedimento abbiano necessità di acquisire la "identità digitale" utilizzata dall'indagato all'interno di piattaforme social o ambienti virtuali: in tale contesto, occorre stabilire se il c.d. *nickname* possa essere ricondotto alla nozione di "generalità" di cui all'art. 66, comma 1, c.p.p., rispetto alla quale egli è tenuto a dichiarare il vero, non

1. Al riguardo, invero, occorre tenere distinte la facoltà di non autoincriminarsi intesa in senso stretto e, cioè di non fornire risposte dalle quali emergano responsabilità per fatti non ancora oggetto di accertamento procedimentale in sede penale, e la facoltà di rimanere in silenzio (facoltà di non autoincriminarsi in senso lato) per evitare di contribuire alla condanna rispetto a un fatto già formalmente addebitato: Chelo 2025, p. 2, nt. 2; Mazza 2004, p. 50, nt. 148.
2. In argomento, v., tra i molti, Amodio 1974; Catalano 2011; Chiavario 1982; Conti 2003; Ferrua 1989; Grevi 1998; Grevi 1972; Illuminati 2012; Illuminati 1999; Illuminati 1993; Mazza 2004; Marafioti 2000; Moscarini 2010; Moscarini 2006; Paladin 1965; Patanè 2006.
3. Di un "corpo elettronico" quale miniera d'oro da cui estrarre dati ha parlato, come noto, Rodotà 2012, p. 322.
4. Per spunti al riguardo, v. Mangiaracina 2021; Parlato 2020.
5. Cfr., *ex multis*, Bontempelli 2018, p. 14; Caprioli 2017, p. 486; Chelo 2025, p. 195 ss.; Chelo 2022; Filippi 2021; Miraglia 2023; Torre 2017, p. 69.

potendo invocare – almeno secondo l'interpretazione prevalente[6] – il diritto al silenzio[7].

Dette operazioni, come appare evidente, presuppongono talora una qualche forma di collaborazione attiva da parte della persona coinvolta, sollevando così interrogativi cruciali circa l'estensione della garanzia in parola e la legittimità di metodologie intrusive che tendono a forzare – anche solo indirettamente – il compimento di condotte autoindizianti. In sintesi: è stato detto – impiegando locuzioni tanto icastiche quanto rivelatrici – che siffatta prerogativa è passata dall'essere percepita come un retaggio del passato, quasi una garanzia da "*boomer*", a diventare uno dei presìdi più attuali della legalità costituzionale, imprescindibile per la moderna "*generazione Alpha*"[8].

Tanto premesso in termini generali, deve osservarsi come il diritto al silenzio – sintetizzato nel brocardo *nemo tenetur se detegere* – rivesta una posizione preminente nel disegno complessivo dei principi che caratterizzano il c.d. *adversarial system*[9], giacché rappresenta, come noto, un ineliminabile corollario del diritto di difesa[10], nonché della presunzione di non colpevolezza[11]. Incontestati e saldi sono i riferimenti normativi – costituzionali e sovranazionali – cui ancorare siffatta garanzia: artt. 13[12], 24, comma 2, 27, comma 2, 111, 117 Cost.[13]; art. 6 CEDU[14]; art. 14, § 3, lett. g), Patto int. dir. civ.; artt. 47, § 2, 48 CDFUE[15].

La sua centralità è legata – anche dal punto di vista storico-giuridico – al rifiuto dell'idea in base alla quale l'imputato dovrebbe ritenersi obbligato a contribuire all'accertamento dei fatti nel procedimento penale a suo carico, in quanto unico conoscitore della verità[16]. Grava, invece, sulla pubblica accusa l'onere di ricercare la prova "[by] *its own independent labors*"[17], ossia senza potersi avvalere della collaborazione coatta del prevenuto. Come sottolineato in dottrina, del resto, la corretta relazione tra individuo e potere pubblico risulterebbe compromessa laddove fosse imposto a quest'ultimo di fornire la propria versione dei fatti (o financo

6. L'art. 64, comma 2, lett. c), c.p.p., infatti, riconosce all'interrogato la facoltà di non rispondere, "salvo quanto disposto dall'art. 66, comma 1"; v., per tutti, Dominioni 1989, p. 411.
7. Cfr. Signorato 2018, p. 34 s., la quale nega l'operatività della garanzia facendo leva su "una lettura evolutiva [del dettato normativo] alla luce della tecnologia". *Contra*, Cesari 2019, p. 1180 s.; Mangiaracina 2021, p. 736.
8. Galantini 2024.
9. Grevi 1972, p. 77; Illuminati 2012, p. 1262. Il principio in parola è stato definito come "la prima massima espressione del garantismo processuale accusatorio": Patanè 2006, p. 1.
10. Carulli 1985, p. 72; Chiavario 2002, p. 145; Cordero 1987, p. 226; Corso 1999, p. 1080; Ferrua 1989, p. 471; Giarda 1980, p. 118; Grevi 2000, p. 205; Grevi 1972, p. 45; Illuminati 2012, p. 1258 ss.; Illuminati 1999, p. 305; Marafioti 2000, p. 29; Patané 2006, p. 81; Scaparone 1980, p. 25.
11. Grevi 1972, p. 12, nt. 17, 46 s.; Illuminati 1979, p. 172 ss.; Patanè 2006, p. 105 ss. Ad avviso di Mazza 2004, p. 46 ss., non è legittimo esigere da chi è presunto innocente un apporto informativo su circostanze che, per principio costituzionale, si devono presumere a lui non conosciute.
12. Vassalli 1997, p. 253 ss.
13. Illuminati 2012, p. 1261, per il quale "il radicamento costituzionale di questo principio è fuori discussione"; Moscarini 2014, p. 27 ss.
14. "The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention": così, Corte EDU, 17 dicembre 1996, *Saunders c. Regno Unito*, par. 68. Cfr. anche Corte EDU, 28 aprile 2022, *Wang c. Francia*; Corte EDU, 20 settembre 2022, *Merahi e Delahaye c. Francia*. In dottrina, v., tra i molti, Catalano 2011, p. 4030; Ubertis 2000, p. 42; Zacché 2008, p. 179.
15. Di Bitonto 2017, p. 2002; Falato 2022; Galantini 2024, p. 1043; Patanè 2024, p. 1999 ss.
16. Giarda 1980, p. 8; Grevi 1972, p. 76.
17. *Miranda c. Arizona*, 384 U.S. 436 (1966).

una confessione) sotto la minaccia di un'inferenza negativa (si legga, *contra se*) dalla sua condotta[18].

Esigenza naturale ancor prima che giuridica, il principio in oggetto, dunque, rivela una portata sistematica destinata a riflettersi sulle regole fondamentali che governano il processo penale: "dalle esigenze della difesa sociale alla tutela della persona dell'imputato; dalla ricorrente tentazione di ripristinare strumenti di acquisizione delle 'fonti' e dei risultati di prova ad impronta inquisitoria, alla sempre più diffusamente sentita necessità di riaffermare, contro, o almeno a fronte, di ogni potere dello Stato taluni insopprimibili diritti dell'uomo"[19].

Non è questa la sede per soffermarsi, *funditus*, sulle numerose, variegate e, alle volte, contraddittorie definizioni offerte in relazione a un concetto che pecca per una singolare vaghezza tanto nei contenuti, quanto nell'ambito applicativo[20]. A conferma della costante "instabilità concettuale"[21], è sufficiente osservare come "tale principio, nelle molteplici varianti della sua formulazione latina, sia stato spesso richiamato con riguardo ad una gamma di comportamenti piuttosto eterogeni"[22]. Esso, come noto, costituisce l'espressione di tre differenti prerogative: il diritto a non essere interrogato (*right not to be questioned*), il diritto a non autoincriminarsi (*privilege against self-incrimination*) e il diritto al silenzio in senso stretto (*right to be in silence*)[23]. Il *nemo tenetur edere contra se*, in questa prospettiva, è stato talvolta riferito alle sole "dichiarazioni verbali o scritte" rese dall'indagato/imputato nel corso del procedimento (tanto in sede istruttoria quanto in sede dibattimentale)[24]; talaltra, alle "condotte collaborative" tenute con l'autorità inquirente (autoincriminanti[25] o anche in senso lato[26]); o, ancora, a un vero e proprio diritto a non collaborare con l'accusa e, dunque, a non contribuire in alcun modo alla dimostrazione della propria colpevolezza (*right not to give evidence*)[27].

18. Greenawal 1974, p. 259; Jackson 2009, p. 360.
19. Giarda 1980, p. 5. Cfr. pure Grevi 2000, p. 203, per il quale il tema del diritto al silenzio è il "riflesso dell'ancora più generale scelta tra concezione autoritaria e concezione liberale del processo"; Mazza 2004, p. 2 s., secondo cui "è proprio questo […] il terreno su cui meglio si possono misurare le scelte culturali, ideologiche e politiche sottostanti ai diversi sistemi processuali e, più in generale, all'assetto dei rapporti intercorrenti in un dato momento storico fra Stato e cittadino, fra 'autorità' e 'libertà'".
20. In generale, sull'evoluzione storica del principio, v. Catalano 2011, p. 4018 ss.; Grevi 1972, p. 1 ss.; Tassinari 2012, p. 15 ss.
21. Green 1999, p. 628 (trad. dell'A.)
22. Grevi 1972, p. 3 s.
23. Su tale classificazione, v., tra i molti, Amodio 1974, p. 412; Di Bitonto 2008, p. 68; Marafioti 2000, p. 115; Patanè 2006, p. 2. Al riguardo, invero, occorre tenere distinte la "facoltà di non autoincriminarsi intesa in senso stretto" e, cioè di non fornire risposte dalle quali emergano responsabilità per fatti non ancora oggetto di procedimento, e la "facoltà di rimanere in silenzio" (facoltà di non autoincriminarsi in senso lato) per evitare di contribuire alla condanna rispetto a un fatto già formalmente addebitato: Mazza 2004, p. 50, nt. 148; Tonini 2002, p. 835.
24. In questo senso, v. Gabrielli 2012, p. 25.
25. Cfr. il considerando n. 25 della direttiva 2016/343/UE, ove si stabilisce che "gli indagati e imputati, se invitati a rilasciare dichiarazioni o a rispondere a domande, non dovrebbero essere costretti a produrre prove o documenti o a fornire informazioni che possano condurre all'autoincriminazione". Si veda anche la Commissione delle Comunità Europee, *Libro verde sulla presunzione di non colpevolezza*, Bruxelles, 2006, COM (2006)17, par. 2.4, in cui ci si riferisce a un diritto "a non essere obbligato a fornire prove di colpevolezza".
26. Manzini 1982, p. 543, per il quale "la libertà dalle autoincriminazioni [garantita all'art. 24, comma 2, Cost.] comprende […] il diritto di non essere costretto a porre in essere alcun comportamento, anche non consistente in dichiarazioni, il quale possa pregiudicare il suo autore nello svolgimento di una difesa nel processo".
27. Corte cost., 6 aprile 2023, n. 111; Corte cost., 30 aprile 2021, n. 84. Per questa visione estensiva, v. Mazza 2014, p. 1409; Munoz Conde 2009, p. 10 s., nella parte in cui allude a un diritto "a non essere obbligato direttamente, coattivamente, o indirettamente, mediante raggiri, a dichiarare la propria colpevolezza o a fornire dati che

A prescindere da come lo si voglia intendere, deve rilevarsi – ed è su questo aspetto che si concentreranno le riflessioni a seguire – come vada affiorando, a più riprese, nella giurisprudenza di legittimità italiana, l'esigenza di circoscrivere l'ambito di applicazione del diritto di autodifesa negativa con particolare riferimento all'impiego delle intercettazioni telefoniche. Ci si riferisce, più precisamente, alla tematica concernente il valore probatorio – e, prima ancora, l'eventuale utilizzabilità – da attribuire alle dichiarazioni autoaccusatorie/confessorie rese dall'indagato nel corso di una captazione previamente e legittimamente autorizzata[28]. Al riguardo, l'orientamento pretorio delineatosi nel corso degli ultimi anni pare granitico: da tempo, in effetti, i giudici vanno affermando che "le dichiarazioni, captate nel corso di attività di intercettazione regolarmente autorizzata, con le quali un soggetto si autoaccusa della commissione di reati hanno integrale valenza probatoria non trovando applicazione al riguardo gli artt. 62 e 63 c.p.p.", in quanto "l'ammissione di circostanze indizianti, fatta spontaneamente dall'indagato […] non è assimilabile alle dichiarazioni da lui rese dinanzi all'autorità giudiziaria o alla polizia giudiziaria"[29].

Preso atto di ciò, pare interessante interrogarsi sui motivi che inducono ciclicamente la Suprema corte ad affrontare siffatta questione. Un quesito sorge, difatti, spontaneo: le pronunce in argomento, lungi dal rappresentare semplici precisazioni interpretative, rivelano forse il permanere di un disagio sistematico, alimentato dall'evoluzione delle tecniche investigative e dalla difficoltà di adattare le garanzie tradizionali (*rectius*, il *nemo tenetur*) ai nuovi scenari probatori informatico-digitali? Si è già detto, del resto, come l'avvento delle nuove Tecnologie dell'Informazione e della Comunicazione (ICT) renda necessario, più in generale, domandarsi "se" e "come" la garanzia del diritto al silenzio debba operare con riguardo a quelle tecniche investigative capaci di coartare, anche solo indirettamente, la volontà del prevenuto.

Al fine di sgomberare il campo da possibili equivoci, è opportuno individuare con maggiore precisione la *quaestio iuris* sulla quale si intende soffermare l'attenzione.

Ciò che rileva, ai fini della presente analisi, non è certo la verifica in ordine all'utilizzabilità di qualunque dichiarazione dell'indagato captata nel corso di un'intercettazione telefonica. È evidente, infatti, che "se si dovesse escludere l'indiziato dal novero delle persone che possono essere intercettate […] ci si chiede a cosa mai potrebbe servire intercettare solo persone non indiziate, posto che attraverso l'intercettazione si cerca per l'appunto di scoprire comunicazioni che valgano a dimostrare la responsabilità del soggetto"[30]. Il punto nevralgico, viceversa, riguarda la possibilità o meno di tacciare come inutilizzabili solo quelle manifestazioni di pensiero con le quali l'indagato si autoaccusa della commissione di un reato (dichiarazioni autoaccusatorie in senso stretto).

In via meramente esemplificativa, pertanto, non si dubita della piena spendibilità procedimentale di propalazioni, pur riferibili al prevenuto, che non sono direttamente espressive del fatto principale di reato ("ci vediamo domani sera al bar in via Rossi"). Oggetto di discussione sono, invece, espressioni con le quali si confida a un amico la realizzazione di un delitto ("ieri ho rubato un cellulare").

2. Fondamento e portata applicativa del diritto al silenzio nelle intercettazioni

Chiariti i termini generali della questione, è possibile rilevare come in letteratura si siano andate

facilitino le indagini relative ad un delitto al quale si presume che il soggetto abbia partecipato"; Scaparone 1980, p. 31, nt. 26; Tassinari 2012, p. 278; Ubertis 2008, p. 435.

28. Cass. pen., Sez. I, 28 marzo 2024, n. 19722, in "OneLegale"; Cass. pen., Sez. II, 12 giugno 2019, n. 37794, *ivi*; Cass. pen., Sez. Un., 26 febbraio 2015, n. 22471, *ivi*; Cass. pen, Sez. VI, 19 febbraio 2013, n. 16165, *ivi*; Cass. pen., Sez. IV, 2 luglio 2010, n. 34807, *ivi*; Cass. pen, Sez. VI, 22 maggio 2003, n. 31739, *ivi*; Cass. pen., Sez. V, 3 maggio 2001, n. 27656, *ivi*; Cass. pen., Sez. VI, 1° febbraio 1994, n. 317, Cuozzo, in *Giust. pen.*, 1994, p. 488.

29. Cass. pen., Sez. II, 12 giugno 2019, n. 37794, cit.

30. Illuminati 2013, p. 102. Ad avviso di Grevi 1971, p. 1070, così operando, "l'ambito di operatività del principio sancito *ex* art. 15 comma 2 Cost. con riguardo alle comunicazioni telefoniche verrebbe a restringersi, in relazione al processo penale, ad una serie di ipotesi assolutamente marginali, in quanto risulterebbero legittime le sole intercettazioni effettuate nei confronti di persone diverse dall'imputato, e nemmeno indiziate o sospettate".

sviluppando due linee interpretative tra loro radicalmente antitetiche. In proposito, è opportuno sottolineare fin da subito – ma si avrà modo di comprovarlo a seguire – come i divergenti approcci riflettano una profonda antinomia circa l'individuazione della *ratio* del brocardo *nemo tenetur se detegere* e del ruolo assunto dall'imputato (*rectius*, delle modalità acquisitive del suo sapere) nell'attuale contesto investigativo-probatorio[31].

2.1. La tesi della spontaneità

La giurisprudenza[32] e la dottrina maggioritaria[33] sostengono che la garanzia del diritto al silenzio non operi allorquando le dichiarazioni *contra se* provenienti dall'indagato siano captate nel corso di un'intercettazione telefonica o telematica legittimamente autorizzata.

La giustificazione offerta muove da un assunto ben preciso: il diritto a non autoincriminarsi – si sostiene – trova applicazione solo in presenza di un contatto diretto e immediato (nel senso di non-mediato da terzi) tra il prevenuto e l'autorità procedente (giudice, pubblico ministero o polizia giudiziaria) nel corso del procedimento penale[34]. Occorre ricordare, d'altro canto, come la *ratio* del principio venga tradizionalmente ricondotta proprio alla necessità di impedire che l'indagato sia in qualunque modo indotto, tramite coartazione fisica o psicologica – da parte degli organi statali – a rendere dichiarazioni autoaccusatorie o, a seconda della lettura che si intenda prediligere, ad agire a proprio danno[35]. È questa, peraltro, la lettura (consolidata) offerta dalla giurisprudenza strasburghese che, pur in assenza di un riferimento esplicito nel testo convenzionale, individua il fondamento della garanzia in parola[36] (ricondotta, come detto, all'art. 6 CEDU) nell'esigenza di protezione dell'accusato "against improper compulsion by the authorities"[37].

L'esegesi che si va esponendo sembra affondare le proprie radici nella celebre opera con la quale autorevole dottrina ebbe modo di affermare, in termini espliciti, che il diritto al silenzio non può operare con riguardo alle propalazioni dell'indagato rese nel corso di un'intercettazione telefonica[38]. In tali casi – si è sostenuto – non vi è alcun pericolo, neppure in astratto, che egli possa essere influenzato o indotto a modificare la propria volontà dichiarativa. Nel corso della captazione, infatti, il bersaglio è ignaro di essere occultamente ascoltato, e proprio questa caratteristica del mezzo di ricerca della prova, per quanto "'odiosa', ed in un certo senso immorale […] consente di distinguere l'ipotesi *de qua* dalle ipotesi cui si riferisce la garanzia del diritto al silenzio nell'attuale ordinamento"[39].

Come noto, le argomentazioni dell'illustre Autore sono state riprese dalla Corte delle Leggi allorquando, l'anno successivo alla pubblicazione del manoscritto appena ricordato, fu rigettata una questione di legittimità costituzionale proprio con riferimento alla violazione degli artt. 15 e 24 Cost., nella parte in cui la disciplina *ex* artt. 266 ss.

31. Cfr., *amplius*, Buzzelli 1990, p. 885 ss.; Marchetti 1994, *passim*.
32. Cfr. *supra* nt. 21.
33. Grevi 2009, p. 28; Grevi 1973, p. 317; Grevi 1971, p. 1067 ss.; Filippi 1997, p. 23 s.; Illuminati 2012, p. 1265; Illuminati 1983, p. 79; Mazza 2004, p. 53 ss.
34. Illuminati 2012, p. 1265. Per questa opinione, v., in una prospettiva più generale, Galantini 1992, p. 193; e, di recente, Miraglia 2023, p. 1232. Con specifico riguardo all'acquisizione di materiale biologico, v. Camon 2014, p. 1443, per il quale se la manovra investigativa "non implica un contatto con l'individuo (come nel caso dell'offerta maliziosa d'una bevanda o d'una sigaretta), allora l'eventuale inganno è irrilevante"; Bonzano 2017, p. 39; Felicioni 2007, p. 59. *Contra*, però, Fanuele 2009, p. 49; Alesci 2017, p. 165 ss.
35. In tal senso, v. Grevi 1971, p. 1068, per il quale la garanzia del diritto al silenzio "riguarda le sole ipotesi in cui l'inquisito si trova di fronte all'autorità (di polizia o giudiziaria), in posizione di più o meno marcata soggezione psicologica". Nella stessa direzione, v. Illuminati 2012, p. 1265; Mazza 2004, p. 53, il quale esclude l'operatività della garanzia in assenza di un "rapporto diretto di soggezione con l'autorità"; Patanè 2006, p. 89.
36. Balsamo 2018, p. 99 ss.
37. Corte EDU, 11 luglio 2006, *Jalloh c. Germania*, par. 100-102; Corte EDU, 10 marzo 2009, *Bykov c. Russia*, par. 92.
38. Grevi 1972, p. 244 s.
39. Grevi 1971, p. 106. Ad avviso di Foschini 1961, p. 60, "è chiaro che trattasi di attività dominata dall'astuzia".

c.p.p. appariva in contrasto con la facoltà di non autoincriminarsi[40]. In quel contesto, la Consulta affermò che lo scopo della garanzia di derivazione anglosassone è quello di "rafforzare la libertà morale dell'imputato per sollevarlo dallo stato di soggezione psicologica in cui possa venire a trovarsi al cospetto dell'autorità e per porlo al riparo da eventuali pressioni che su di lui possano essere esercitate"[41].

Di conseguenza, nel caso di attività intercettativa, trattandosi di captazione fraudolenta di dichiarazioni spontanee verso un terzo interlocutore, non vi è alcun timore che la volontà del dichiarante possa essere inquinata o coartata dall'autorità procedente. Essa non si palesa come tale, né impiega sotterfugi onde acquisire il contributo dell'indagato. Nessuna esigenza di tutela della libertà morale del prevenuto può essere, dunque, fondatamente invocata. Egli, pur contribuendo attivamente (*facere*) all'emersione di prove *contra se*, sceglie liberamente di condividere il proprio patrimonio conoscitivo con terzi, nella piena in-consapevolezza del fatto che quella manifestazione di pensiero sia ascoltata *live* e registrata dall'autorità inquirente.

Collocandosi in questa prospettiva, dunque, dovrebbe emergere ancor più nitidamente la stretta contiguità tra il *nemo tenetur se ipsum prodere* e la necessità che si vada delineando, ai fini dell'attivazione della garanzia, una relazione *de visu* tra l'indagato e il potere pubblico: "solo in relazione alle ipotesi in cui si instauri un rapporto dialettico diretto tra l'organo inquirente e la persona sottoposta a procedimento"[42] potrà invocarsi la tutela ricavabile dall'art. 24, comma 2, Cost.

In termini più specifici, sembra potersi affermare che l'impostazione in esame subordini l'operatività della garanzia alla "spontaneità" della dichiarazione[43]. Secondo questa lettura, infatti, il valore oggetto di tutela del *nemo tenetur* va individuato nella libertà di autodeterminazione della persona, nel senso che questa deve poter scegliere liberamente e senza costrizione alcuna, se tenere o meno una condotta collaborativa rispetto ad eventuali "richieste" provenienti dagli organi del procedimento.

2.2. La tesi della consapevolezza: critiche

A questo primo filone interpretativo si è vivacemente contrapposta, come anticipato, una diversa e autorevole lettura che – seppur isolata – ha messo in luce come la sfera applicativa del diritto di non autoincriminarsi debba essere estesa anche alle dichiarazioni autoaccusatorie occultamente captate[44].

Questa linea di pensiero, a ben vedere, parrebbe impostare i termini del problema muovendo da una vera e propria "destrutturazione" della *ratio* storica del principio in esame. Si sostiene, più precisamente, che, onde garantirne piena effettività, non è sufficiente tutelare l'indagato dal pericolo di una contaminazione esterna della sua volontà e renderlo edotto circa la possibilità di avvalersi del diritto al silenzio; occorre, altresì, che egli sia pienamente "consapevole" che le dichiarazioni da lui rese nel corso dell'*iter* procedimentale possono essere utilizzate a proprio carico.

In termini più generali, sembra che la tesi in esame approcci il tema muovendo dal seguente postulato: gli apporti conoscitivi (autoaccusatori) provenienti dall'imputato legittimamente utilizzabili solo sono quelli "spontane[i], coscienti e libera espressione di una volontà di leale collaborazione"[45]. Ciò che rileva allorquando si discute dell'ambito applicativo del *nemo tenetur se detegere*, pertanto, non è la spontaneità o la genuinità della propalazione orale o reale (ossia l'assenza di costrizione o inganno ad opera dell'autorità), bensì, lo si ripete, la consapevolezza – in capo al prevenuto

40. Cfr. Corte cost., 4 aprile 1973, n. 34, sulla quale, v. Grevi 1973, p. 317 ss.
41. Cfr. Corte cost., 4 aprile 1973, n. 34, cit.
42. Grevi 2009, p. 28; Grevi 1972, p. 245.
43. Grevi 1972, p. 11 s., ove ricollega l'affermarsi di tale principio alla "forte esigenza di garanzie per la spontaneità dei meccanismi di autodeterminazione dell'individuo".
44. È l'opinione sostenuta da Giarda 2007, p. 11 ss.
45. Giarda 1980, p. 9.

– che quest'ultima possa essere utilizzata come prova di penale responsabilità[46].

Un tanto troverebbe conferma – secondo questa impostazione – nella disciplina degli avvisi preliminari di cui all'art. 64 c.p.p.: ogniqualvolta l'indagato rende dichiarazioni di scienza nel corso del procedimento – indipendentemente dalla fase – il codice di rito prevede l'obbligo di rendere consapevole quest'ultimo del loro impiego probatorio. Scorrendo le norme codicistiche che disciplinano il rapporto fra indagato ed autorità pubblica (quali, ad esempio, gli artt. 64, 350, 386, 388, 391, 374, 421 c.p.p.) ci si accorge come, in tutti questi casi, non solo egli risulti titolare della facoltà di non rispondere – e di tale deve essere avvisato – ma pure che deve essere cosciente degli effetti processuali della sua condotta collaborativa[47].

Al fine di escludere qualunque utilizzo del materiale probatorio *contra se* così raccolto, la dottrina qui in esame propone diverse soluzioni.

La prima opzione è quella di un intervento legislativo volto ad introdurre un'ulteriore ipotesi di inutilizzabilità speciale. Il nuovo ed ipotetico comma 1-*bis* dell'art. 271 c.p.p. potrebbe esprimersi in questi termini: "sono altresì inutilizzabili le dichiarazioni intercettate nel corso di una captazione con le quali l'indagato si autoaccusa espressamente della commissione di un reato".

D'altro canto, sarebbe altresì ipotizzabile un giudizio di legittimità costituzionale con riferimento all'art. 271 c.p.p.[48]. Le norme a tale scopo invocabili sarebbero essenzialmente due.

In primo luogo, l'art. 24, comma 2, Cost., riferimento costituzionale dello *ius tacendi* che impone, quale conseguenza necessaria del suo riconoscimento, l'irrinunciabilità di tale garanzia. Sicché, nel caso delle intercettazioni, la natura fraudolenta del mezzo, comportando una rinuncia obbligata alla prerogativa in questione, non consente all'indagato di scegliere se e come contribuire all'accertamento della propria responsabilità.

In secondo luogo, si è fatto notare come l'attuale disciplina delle intercettazioni non si adegui neppure al canone sancito all'art. 3 Cost. In sostanza, vi sarebbe un'indebita differenziazione nei mezzi difensivi fra l'indagato che si confronta direttamente con l'organo inquirente e colui che, invece, viene intercettato fraudolentemente: solo il primo, in quanto destinatario dell'avviso, potrà avere la piena consapevolezza della sorte processuale della sua eventuale condotta collaborativa[49].

Sennonché, quest'ultima argomentazione – pur suggestiva – dovrebbe essere smorzata dalla considerazione per cui il principio di eguaglianza, nella sua dimensione sostanziale, impone di trattare diversamente situazioni differenti fra loro. Si vuol dire, in altri termini, che le modalità di apprensione del materiale conoscitivo proveniente dall'indagato si distinguono quanto alla peculiarità del mezzo acquisitivo (dichiarazione diretta all'autorità pubblica, da un lato, ed intercettazione, dall'altro). Ma, se è da ritenersi certamente legittimo l'utilizzo delle intercettazioni ove siano rispettati i criteri di cui all'art. 15 Cost., il differente regime di trattamento parrebbe legittimo.

In terzo luogo, onde avvalorare la lettura minoritaria, potrebbe astrattamente invocarsi il contenuto dell'art. 188 c.p.p., disposizione codicistica volta a tutelare la libertà morale della persona nei cui confronti è diretta l'attività probatoria[50]. Onde renderla operativa nell'ipotesi in esame, occorrerebbe, all'evidenza, muovere da un'accezione ampia del concetto *de quo*, presupponendo che l'autodeterminazione del soggetto sia lesa tutte le volte in

46. Giarda 2007, p. 11: "non ci può essere nel sistema costituzionale del processo penale spazio perché le dichiarazioni autoaccusatorie dell'imputato siano acquisite con metodi, tecniche, istituti giuridici o prassi operative che non riconoscano all'imputato stesso il diritto preliminare ed inviolabile di rendersi conto e di scegliere consapevolmente se fare o non fare dichiarazioni autoaccusatorie, collaborando così con gli inquirenti, in piena ed assoluta autonomia decisionale […]. L'imputato o l'indagato deve essere consapevole nel fare dichiarazioni autoaccusatorie di trovarsi di fronte ad un soggetto che, raccogliendole opportunamente a verbale, le potrà utilizzare anche contro di lui".

47. *Ivi*, p. 12.

48. *Ibidem*.

49. *Ibidem*.

50. Grevi 1972, p. 245. Sulla portata sistematica di tale disposizione, v., di recente, Chelo 2025.

cui l'interessato non ha la piena consapevolezza di essere coinvolto nell'esecuzione di un atto di indagine[51]. È solo in tal modo, infatti, che la volontà potrà dirsi "formata" senza costrizioni, né intromissioni esterne.

Epperò, il ricorso a un'interpretazione come quella appena ipotizzata sembrerebbe destare qualche riserva.

In effetti, se il fine ultimo della norma è quello di vietare il ricorso a "ogni espediente psico-compulsivo"[52], non si comprende come una semplice captazione occulta effettuata da remoto possa incidere sul percorso di formazione della volontà: l'autorità inquirente non realizza alcuna forma di violenza, minaccia o inganno nei confronti del destinatario della misura. Ciò che occorre davvero garantire – onde rendere concreta la libertà di poter "determinare il proprio comportamento senza esterne imposizioni"[53] – non è tanto, quindi, la consapevolezza della realtà circostante, bensì la spontaneità del comportamento collaborativo, ovverosia l'assenza di un impulso esterno idoneo a influire sul processo decisionale. E del resto, la giurisprudenza di legittimità, quando si è soffermata sul rapporto fra libertà morale ed intercettazioni, ha comunque ritenuto inutilizzabili solo quelle dichiarazioni che siano state "indotte" da parte degli organi inquirenti[54].

Ma vieppiù.

Oltre a quanto appena rilevato, la tesi in esame è avversata anche con riguardo a ulteriori profili, taluni dei quali meritano qualche precisazione.

Innanzitutto, autorevoli commentatori[55] – in linea con varie pronunce di legittimità[56] – hanno messo in luce la distinzione tra "dichiarazione come atto del procedimento" e "conversazione captata con l'intercettazione": mentre la prima, costituendo una vera e propria manifestazione volitiva di scienza con la quale l'indagato offre il proprio contributo al processo, è coperta dallo *ius tacendi*, la seconda, viceversa, non costituisce la "narrazione di un fatto", bensì un "atto

51. Sembra collocarsi in questa prospettiva, Patanè 2006, p. 103 s., per la quale l'apporto dell'indagato "alla ricostruzione del fatto deve essere frutto di un'iniziativa informata, consapevole e spontanea rispetto alla vicenda processuale". Su questa stessa linea di pensiero, v., con riguardo al tema del prelievo "ingannevole" di reperti biologici, Fanuele 2009, p. 49 e, in merito all'impiego di stratagemmi per consentire l'intercettazione nel domicilio, Filippi 1997, p. 59, secondo cui "il titolare della libertà domiciliare, se avesse conosciuto il reale scopo dell'immissione, non avrebbe prestato il consenso, il quale è quindi viziato e *tamquam non esset*". Di recente, v. anche Chelo 2025, p. 93 ss.

52. Cordero 2012, p. 616.

53. Vassalli 1997, p. 289. L'A., più precisamente, identifica il contenuto del diritto di autodeterminarsi nella "libertà di non vedere né ingannata né coartata la propria coscienza, il diritto a non vedersi ingiustamente imposto un determinato contegno, neanche passivo o inerte, il diritto infine […] a formare con motivi propri le proprie determinazioni" (pp. 306-307). In termini non dissimili, v. Scomparin 2002, p. 2, ove l'A. si riferisce alla libertà "di formare senza costrizioni la propria volontà e di muovere il proprio comportamento esteriore in conformità alle spinte psichiche interne, senza intromissioni e senza la sottoposizione coatta ad introspezioni che ne svelino il concreto funzionamento»; Patanè 2006, p. 102, in cui si definisce la libertà morale come "libertà del singolo […] di agire in conformità alle spinte psichiche interne".

54. Cass. pen., Sez. I, 18 dicembre 2013, n. 4429, in "OneLegale", ove si precisa che "è inutilizzabile l'intercettazione delle dichiarazioni indotte in una persona dall'adozione di metodi o tecniche idonei a influire sulla sua capacità di autodeterminazione, posto che il divieto dell'art. 188, primo comma, c.p.p. investe l'oggetto della prova e non è circoscritto al contesto formale delle sole prove dichiarative".

55. Illuminati 1983, p. 80.

56. Cass. pen., Sez. II, 15 maggio 2012, n. 31064, in "OneLegale": "le intercettazioni (art. 266 c.p.p.) non hanno per oggetto le dichiarazioni, ma le 'conversazioni o comunicazioni' termini che individuano attività ben diverse dalle dichiarazioni". Pertanto, "nel caso regolato dagli artt. 266 e ss. c.p.p. i soggetti intercettati non sanno di essere indagati ed evidentemente non rilasciano dichiarazioni reciproche, ma semplicemente conversano ignorando di essere sottoposti ad intercettazione".

performativo"[57] e, cioè, una *res gestae*. Alla luce di tale classificazione, pertanto, si afferma che la confessione resa nel corso di un'intercettazione telefonica si identifica con la semplice trascrizione di un'azione (*rectius*, di un fatto storico), non potendo essere in alcun modo assimilabile ad una "dichiarazione" resa nel procedimento. La critica intende evidentemente escludere dal novero delle attività coperte dalla garanzia quelle propalazioni *contra se* rese contestualmente allo svolgimento di un'attività illecita.

Sennonché, tale ragionamento potrebbe risultare difficilmente compatibile con le dichiarazioni autoindizianti che non siano accompagnate, nella loro immediatezza, da una condotta penalmente rilevante. A quest'ultimo proposito, non può non osservarsi come il formante dichiarativo, proprio di una qualunque manifestazione di volontà, si adatti diversamente a seconda dell'oggetto della stessa. Se rispetto ad una qualunque esternazione del prevenuto oggetto di intercettazione appare fondato sostenere che si tratti di un fatto storico, più complesso, invece, è riuscire ad eliminare del tutto il formante dichiarativo allorquando, nel corso della captazione, egli, affermando la propria colpevolezza, non accompagni tale dichiarazione con il compimento di un atto – direttamente o indirettamente – espressivo del fatto oggetto di imputazione. In quest'ultimo caso, la portata di quell'atto performativo, è espressione del reato. Ed allora, quale sarebbe la differenza tra la dichiarazione di scienza resa davanti all'autorità procedente e l'autoaccusa captata nel corso di un'intercettazione?

Ferme tali considerazioni, la tesi minoritaria può essere censurata anche sotto un profilo di carattere sistematico.

Occorre, a tal fine, tenere presente la tradizionale distinzione relativa al *modus partecipandi* dell'accusato all'attività investigativa, ovverosia quale "organo" o quale "oggetto" di prova[58]. Con la prima locuzione si allude all'insieme delle facoltà attribuite all'indagato – espressione del diritto di autodifesa – con cui egli apporta volontariamente, coscientemente e in maniera attiva un contributo conoscitivo al processo. Quanto alla seconda, per contro, egli viene in considerazione come mero oggetto dell'osservazione giudiziale, assumendo in tal modo la qualifica di soggetto passivo dell'accertamento. Il differente ruolo ricoperto dall'indagato nelle due ipotesi incide sul campo di applicazione del diritto al silenzio: quest'ultimo può (e deve) operare solo qualora l'interessato esprima un contributo attivo nell'istruzione probatoria[59].

Calando questa distinzione nell'ambito delle intercettazioni, potrebbe sostenersi – collocandosi nel solco tracciato della tesi minoritaria – che l'indagato realizzi una condotta proattiva, perlomeno qualora si interpreti il concetto di "soggetto di prova" in senso ampio, ossia riferendolo a tutti gli apporti conoscitivi provenienti dall'imputato non coercibili. Sicché, quest'ultimo, in quanto organo di prova, dovrebbe essere necessariamente consapevole della sua posizione, al fine di poter scegliere se tenere o meno una certa condotta collaborativa.

A tale argomentazione, tuttavia, si dovrebbe replicare – richiamando la *ratio* del principio *nemo tenetur se detegere* – che la relativa garanzia è destinata ad operare unicamente nei casi in cui vi sia un concreto rischio di indebita coazione all'autoincriminazione; rischio che, tuttavia, non ricorre, come si è visto, nel caso in cui la dichiarazione dell'indagato sia oggetto di intercettazione.

Al netto di quanto fin ora osservato, le considerazioni da ultimo svolte impongono alcune riflessioni circa uno dei pilastri dogmatici a fondamento dell'istituto della confessione.

Quest'ultima, come risaputo, può essere di due tipi: giudiziale o stragiudiziale[60]. Nel primo caso, vi è una dichiarazione resa dall'indagato-imputato dinnanzi all'autorità inquirente o giudicante (ossia

57. Con l'espressione atto performativo si fa riferimento a quelle "enunciazioni (e per estensione anche di enunciati e di verbi) che non descrivono un'azione né constatano un fatto, bensì coincidono, in determinati contesti, con l'azione stessa", quali, ad esempio, "prendo te come mia sposa": cfr., per la definizione, www.treccani.it.

58. La messa a punto di tale classificazione si deve, come noto, a Florian 1924, p. 9. Cfr. anche Cavallari 1968, p. 180; Dominioni 1985, p. 198 ss.; Felicioni 2007, p. 33.

59. Tonini-Conti 2014, p. 188.

60. Bellavista 1961, p. 919 ss.; Lupària 2006, p. 160; Macchia 1989, p. 25 ss.; Montalbano 1958.

nelle sedi specificatamente "deputate dal legislatore all'acquisizione del [suo] sapere"[61]) e contenente affermazioni a lui astrattamente pregiudizievoli in ordine a una fattispecie penale. Nel secondo caso, invece, la *contra se declaratio* è resa a un soggetto diverso dagli organi procedenti.

Ebbene, ciò che rileva, onde distinguere le diverse tipologie confessorie, non è, pertanto, il momento in cui esse sono rese (cioè, "nel corso" ovvero "prima" dell'instaurarsi del procedimento penale), bensì il soggetto al quale la manifestazione autoaccusatoria è indirizzata. Ne consegue che, laddove la propalazione sia captata nel corso di un'intercettazione, benché formalmente resa nell'ambito di un atto tipico del procedimento, essa assume la natura di confessione stragiudiziale, in quanto rivolta a un terzo-privato.

Concludere in tal senso non è privo di conseguenze ai fini della presente indagine.

La miglior dottrina, infatti, ritiene che una componente fondamentale della confessione giudiziale vada identificata nella "consapevolezza"[62] che la dichiarazione avrà conseguenze sul piano processuale; conseguenze da intendersi, non tanto come volontà della condanna – che, evidentemente, non dipende dall'imputato – bensì come volontà di produrre effetti pregiudizievoli nei propri confronti (così si legge: "consapevolezza degli astratti risvolti processuali dell'asserzione")[63]. È ben vero, dunque, che l'elemento (soggettivo) della consapevolezza assume spessore allorquando si discute della fattispecie confessionale; esso, però, viene in rilievo solamente con riguardo al caso in cui la propalazione *contra se* sia resa dinnanzi all'autorità procedente (confessione giudiziale) e non anche laddove essa sia captata occultamente (confessione stragiudiziale).

3. Le conseguenze processuali dell'utilizzabilità della c.d. confessione intercettata

Volendo accogliere, per le ragioni poc'anzi esposte, l'impostazione maggioritaria – e, quindi, negare rilevanza allo *ius tacendi* nelle ipotesi di dichiarazioni autoaccusatorie legittimamente intercettate –, occorre soffermarsi sulla valenza probatoria di tali propalazioni. È necessario, più precisamente, domandarsi se esse costituiscano rappresentazioni dirette del fatto principale oggetto di imputazione ovvero prove indirette-critiche. L'interrogativo, come ben si intuisce, non è di poco momento: qualificarle alla stregua di meri indizi importa la necessaria applicazione dei parametri di cui all'art. 192, comma 2 c.p.p.[64], i quali, come noto, pongono un limite al ragionamento deduttivo del giudice (e al suo libero convincimento)[65] quando voglia trarre la certezza del noto dall'ignoto[66]; in caso contrario, egli sarà libero di valutarle secondo il proprio convincimento. Per provare a rispondere al quesito è necessario muovere da una considerazione di carattere più generale.

Non potendosi soffermare sull'annoso dibattito in merito alla distinzione tra prove e indizi[67], si ritiene, in premessa, di dover aderire a quell'autorevole orientamento dottrinale che equipara siffatte categorie. Come è stato osservato, "l'ipotesi che qualcosa possa essere 'provato' da entità diverse dalle prove – comunque le si chiami, elementi, indizi, ecc. – è una contraddizione in termini; se x è provato da y, y non può che essere una prova"[68].

61. Lupària 2006, p. 109, quali, ad esempio, l'interrogatorio, il confronto, etc.
62. *Ivi*, p. 106.
63. *Ivi*, p. 107.
64. Il quesito, invero, potrebbe apparire irrilevante allorquando si intenda accogliere quella tesi in base alla quale "tutto è indizio" e "nessun mezzo di prova dispensa dalla verifica", di talché, "la regola espressa nell'art. 192 commi 1 e 2 ha in realtà una portata generale: invero, qualsiasi prova – dalla confessione alla testimonianza – deve essere riscontrata": Fassone 1989, p. 844. Cfr. pure Iacoviello 1997, p. 177.
65. Lozzi 2006, p. 210 ss.
66. Cass. pen., Sez. III, 7 novembre 2023, n. 10683.
67. Si vedano, per tutti, Catalano 2008, p. 794 ss.; Melchionda 1997, p. 664 ss.
68. Ferrua 2018, p. 91. Cfr. pure Ferrua 2020, p. 5, nt. 12, secondo cui "che gli indizi menzionati nell'art. 192 comma 2 c.p.p. costituiscano 'prove' è di tutta evidenza, altrimenti non potrebbero provare alcunché, fossero pure mille, gravi, precisi e concordanti".

Di conseguenza, il riferimento operato dall'art. 192, comma 2, c.p.p. alla gravità, alla precisione e alla concordanza consente di estrapolare dalla disposizione niente più che un semplice "criterio di valutazione relativo al valore, al significato che gli indizi, *rectius* le "prove indiziarie" possono assumere in ordine alla proposizione da provare"[69].

Tanto premesso, è necessario ricordare come le pronunce giurisprudenziali che affrontano il tema in esame siano solite affermare che le dichiarazioni, captate nel corso di attività intercettative, con le quali un soggetto si accusa della commissione di reati hanno "integrale valenza probatoria"[70]. Allo stesso tempo, però, è dato leggere che, in dette ipotesi, non trovano applicazione gli artt. 62 e 63 c.p.p., in quanto le "ammissioni di circostanze indizianti" non sono assimilabili alle enunciazioni rese nel corso dell'interrogatorio dinanzi all'autorità procedente[71].

Ad un prima lettura, l'espressione "integrale valenza probatoria" sembrerebbe alludere alla possibilità, per il giudicante, di valutare il contegno confessorio alla luce del principio del libero convincimento *ex* art. 192, comma 1, c.p.p. Sennonché, il contestuale richiamo "all'ammissione di circostanze indizianti" sembrerebbe indurre, all'opposto, verso una qualificazione delle propalazioni *contra se* alla stregua di mere prove indiziarie, sottoposte, perciò, al criterio "rafforzato" di cui all'art. 192, comma 2 c.p.p.

È su questo aspetto che occorre tentare di fare chiarezza.

Prima facie potrebbe sostenersi che le statuizioni pretorie poc'anzi richiamate non siano affatto in contraddizione tra loro. Allorquando si accolga l'idea che l'indizio è una prova a tutti gli effetti, affermare che l'autoaccusa "ha integrale valenza probatoria" significa semplicemente ribadire che quella "circostanza indiziante" costituisce una vera e propria "prova".

Epperò, una siffatta spiegazione, non solo non appare risolutiva, ma sembra essere smentita dalla stessa giurisprudenza di legittimità.

Nell'esaminare più approfonditamente i suddetti arresti, infatti, ci si imbatte in affermazioni, alquanto lapidarie (ma senz'altro condivisibili), stando alle quali "l'autoaccusa […] non può essere definita alla stregua di semplice ed isolato 'indizio', sì da ritenere non realizzato il criterio valutativo ex art. 192 comma 2 c.p.p."[72]. Ed in effetti, l'indizio – secondo la prospettazione accolta dalla stessa Suprema corte – "è un elemento che per sua stessa natura non è mai 'direttamente' significativo del fatto da provare, siccome ha bisogno di 'combinarsi' con altri elementi di identica indiretta valenza dimostrativa per sfociare nella piena prova"[73].

Se un tanto è vero, appare evidente come la dichiarazione confessoria resa dal prevenuto (pure nel corso di un'intercettazione telefonica) non possa in nessun caso essere accostata ad un indizio, giacché essa, per sua stessa natura, "punta direttamente sul fatto [principale oggetto di imputazione] e lo disvela nella sua pienezza"[74].

Siffatta conclusione risulta avallata pure da una considerazione di carattere sistematico.

Come insegna, nuovamente, l'autorevole dottrina *supra* richiamata, la registrazione del dialogo operata dallo strumento captativo costituisce la

69. Ferrua 2018, p. 92, ove si precisa altresì che "negare natura di prova agli indizi equivale a confondere la prova, come dato valutabile, con la questione del valore che in concreto può assumere". Lo stesso A. osserva come "la prova critico-indiziaria è concettualmente ben definita, ma in nessun modo può contrapporsi alla prova dichiarativa per una minore attendibilità" (Ferrua 2005, p. 361).

70. Cass. pen., Sez. I, 28 marzo 2024, n. 19722, cit.

71. Cfr. *supra* nt. 21.

72. Cfr. *supra* nt. 21.

73. Cass. pen., Sez. V, 3 maggio 2001, n. 27656, cit.

74. Cass. pen., Sez. V, 3 maggio 2001, n. 27656, cit. In senso conforme, v. Cass. pen., Sez. V, 21 febbraio 2014, n. 16397, in "OneLegale". Peraltro, nelle stesse sentenze si legge che "se si considera che la cd. 'chiamata in correità' (art. 192 co. 3 c.p.p.) viene considerata una vera e propria prova, avendo solo bisogno di altri 'elementi di prova che ne confermino l'attendibilità', non può negarsi una valenza probatoria inferiore all'autoaccusa captata in una spontanea conversazione tra presenti, ovviamente ritualmente autorizzata". In tal senso, nella giurisprudenza di merito, si veda, da ultimo, Tribunale Bari, 5 giugno 2019, in "Dejure".

prova critica diretta dell'avvenuta conversazione. In sintesi: "la traccia […] è l'effetto della conversazione che si è svolta; e, poiché questa, come evento del passato, non è più disponibile, la riproduzione sonora (o visiva) ne diventa la prova"[75].

Più complesso è, invece, comprendere quale sia il legame, dal punto di vista probatorio, tra la conversazione intercettata (provata, in via critica, dalla registrazione) e il contenuto del dialogo captato.

A tal fine, si muova dalla seguente considerazione.

Come noto, le diverse tipologie probatorie possono combinarsi fra loro, e proprio il caso dell'intercettazione rientra in quella che è stata definita una "sequenza di prove", cioè l'ipotesi in cui "la prima proposizione provata diventa premessa probatoria rispetto ad una nuova proposizione da provare"[76]. Nella captazione, infatti, la prova critico-indiziaria si combina con una dichiarazione di prova: "la registrazione (prova critico-indiziaria) di un dialogo (prova dichiarativa)"[77]. Detto altrimenti, la conversazione, che è provata per via indiziaria dal nastro magnetico che contiene il dialogo, è, a sua volta, la prova rappresentativa-dichiarativa di ciò che in esso viene affermato.

Poste tali coordinate, non resta che valutare come siffatto ibridismo si rifletta sul campo oggetto della presente trattazione.

Si ipotizzi che il fatto oggetto di prova, il c.d. fatto da provare, sia la proposizione finale principale, e cioè la colpevolezza dell'imputato che, per comodità, può denominarsi X. Ora, per provare il fatto X, può farsi ricorso, come risaputo, a due diverse modalità probatorie.

La prima – prova storica o rappresentativa – consiste nel ragionamento che da un fatto noto ricava, per rappresentazione, il fatto da provare[78]. In questo caso, l'affermazione "contiene già in sé la descrizione del fatto da provare"[79], ovverosia, la colpevolezza dell'imputato.

La seconda, invece, consta nel dimostrare "un qualsiasi altro fatto Y, diverso dalla narrazione di X, dal quale si possa, mediante un ragionamento critico, fondato sulla scienza o sull'esperienza corrente, indurre il fatto X"[80]. In quest'ultima evenienza, la prova ha natura critico-indiziaria perché "la proposizione da provare è inespressa e va individuata con un'attività di decifrazione, più o meno complessa, che implica competenze di tipo empirico, tratte dalla scienza e dall'esperienza corrente"[81].

Cercando di calare queste categorie nell'ipotesi in esame, sembra potersi affermare che qualora l'indagato si limiti, nel corso di una conversazione legittimamente intercettata, a utilizzare espressioni non direttamente rappresentative della propria colpevolezza (quali, ad esempio, "ci vediamo venerdì al porto") l'elemento critico prevalga su quello dichiarativo, giacché egli, in buona sostanza, si "limita a fornire la rappresentazione di un fatto diverso da quello da provare, al quale il primo può far risalire soltanto attraverso mediazioni ulteriori di leggi scientifiche o di "massime di esperienza"[82]. Ne consegue che il giudice ben potrà utilizzare quel contributo conoscitivo, desumendo da esso, secondo i canoni dell'art. 192, comma 2 c.p.p., che l'indagato si stesse riferendo al reato oggetto di imputazione (il fatto X)[83].

75. Così, Ferrua 2018, p. 104, il quale soggiunge che, "quanto al supporto magnetico, su cui è registrata la conversazione, è prova critico-indiziaria, formata in sede processuale, della conversazione stessa". Inoltre, l'intercettazione, sempre con riferimento all'avvenuto dialogo captato, può classificarsi, altresì, come prova critica diretta e costituita: "e così un'intercettazione tra N e P che raccontano y è prova diretta quanto al dialogo tra N e P" (p. 94).
76. Ferrua 2018, p. 106; Pansini 2018, p. 97.
77. Ferrua 2018, p. 106.
78. Nobili 1989, p. 170; Tonini-Conti 2024, p. 249; Ubertis 1995, p. 12.
79. Ferrua 2018, p. 97. Cfr. pure Pansini 2018, p. 22.
80. Ferrua 2018, p. 97.
81. *Ibidem*; Nobili 1989, p. 170 s.
82. Detto altrimenti, "tutto ciò che, pur essendo rilevante ai fini del fatto da provare, non si riduce all'atto comunicativo che lo descrive, che lo notifica, è prova critica": Ferrua 2005, p. 360.
83. Cass. pen., Sez. II, 12 giugno 2019, n. 37794, cit.: "in tema di valutazione della prova, gli indizi raccolti nel corso delle intercettazioni telefoniche possono costituire fonte diretta di prova della colpevolezza dell'imputato e non

Appare, invece, significativamente diverso il caso in cui il prevenuto, nel corso della captazione, si autoattribuisca direttamente la commissione del fatto principale (cioè, del fatto di reato): in tale circostanza, il fattore dichiarativo si impone sull'elemento indiziante, perlomeno per un duplice ordine di ragioni.

In primo luogo, la dichiarazione *contra se* descrive direttamente il fatto ultimo da provare e, cioè, la colpevolezza (caratteristica quest'ultima propria solo della prova dichiarativa e non anche di quella indiretta)[84].

In secondo luogo, la nozione di prova logica/indiziaria – così per come tradizionalmente intesa – impone che da un fatto provato, c.d. circostanza indiziante, si ricavi, per via critica, un fatto da provare *ex* art. 187 c.p.p. Sicché, assimilare la dichiarazione confessoria e la prova critica condurrebbe a un assurdo logico: il fatto noto (la circostanza indiziante: "domenica scorsa ho rubato un diamante") coincide con il fatto da provare (la proposizione finale principale: il reato di furto) in evidente violazione dell'assunto secondo cui "il procedimento indiziario deve muovere da premesse certe, nel senso che devono corrispondere a circostanze fattuali non dubbie e quindi, non consistenti in mere ipotesi o congetture ovvero in giudizi di verosimiglianza"[85].

La conclusione alla quale si è pervenuti, peraltro, risulta indirettamente avvalorata dall'esame della giurisprudenza di legittimità formatasi in tema di c.d. chiamata di correo telefonica, ossia il caso in cui l'indagato accusi telefonicamente un terzo della commissione di un reato, al quale egli stesso dichiara di aver partecipato[86]. Premesso che, dato il carattere occulto dello strumento, non si pone – ad avviso della Corte di cassazione – alcuna esigenza di valutare con maggior rigore la genuinità delle dichiarazioni eteroaccusatorie (*rectius*, non trova applicazione l'art. 192, comma 3, c.p.p.)[87], si

devono necessariamente trovare riscontro in altri elementi esterni qualora siano: a) gravi, cioè consistenti e resistenti alle obiezioni e quindi attendibili e convincenti; b) precisi e non equivoci, cioè non generici e non suscettibili di diversa interpretazione altrettanto verosimile; c) concordanti, cioè non contrastanti tra loro e, più ancora, con altri dati o elementi certi con riferimenti ai risultati delle intercettazioni di comunicazioni". Conforme, Cass. pen., Sez. VI, 4 novembre 2011, n. 3882, in "OneLegale".

84. Gianturco 1958, p. 115; Lupària 2006, p. 205.

85. Cfr. Cass. pen., Sez. II, 29 maggio 2019, n. 26604, in "OneLegale". In tal senso, nella dottrina, Angeletti 2021, p. 138; Tonini 2000, p. 202.

86. Cfr., fra le molte, Cass. pen., Sez. II, 12 giugno 2019, n. 37794, cit.; Cass. pen., Sez. V, 26 marzo 2010, n. 21878, in "OneLegale"; Cass. pen., Sez. IV, 28 settembre 2006, n. 35860, *ivi*.

87. Il chiamante in correità – si afferma – è persona che, interrogata da un giudice o dagli organi inquirenti, accusa altre persone di avere commesso reati, quali che siano le motivazioni che spingono a tali dichiarazioni, non potendosi escludere che esse siano dettate da fini calunniatori o tendenti ad intercettare la legislazione premiale prevista per il fenomeno del c.d. pentitismo: sicché si impone il massimo rigore valutativo, alla luce del canone ermeneutico indicato dall'art. 192, comma 3, c.p.p. Viceversa, i conversanti captati nel corso di un'intercettazione, ignari di essere ascoltati dall'autorità giudiziaria, non scelgono deliberatamente di accusare qualcuno e, dunque, non si pone alcuna esigenza di valutare, con maggior severità, la bontà delle loro dichiarazioni. Cfr., fra le molte, Cass. pen., Sez. I, 28 marzo 2024, n. 19722, cit., nella quale si legge che "le dichiarazioni auto ed etero accusatorie registrate nel corso di attività di intercettazione regolarmente autorizzata hanno piena valenza probatoria e, pur dovendo essere attentamente interpretate e valutate, non necessitano degli elementi di corroborazione previsti dall'art. 192, comma terzo, cod. proc. pen."; Cass. pen., Sez. II, 12 giugno 2019, n. 37794, cit.; Cass. pen., Sez. Un., 26 febbraio 2015, n. 22471, cit., ove si precisa che "la consolidata giurisprudenza di questa Corte ha chiarito, da oltre un decennio (cfr. Sez. 5, n. 13614 del 19/01/2001, Primerano, Rv. 218392 e, da ultimo, Sez. 2, n. 4976 del 12/01/2012, Soriano, Rv. 251812), che le dichiarazioni captate nel corso di attività di intercettazione (regolarmente autorizzata, ovviamente), con le quali un soggetto accusa sé stesso e/o altri della commissione di reati hanno integrale valenza probatoria e non necessitano quindi di ulteriori elementi di corroborazione ai sensi dell'art. 192 c.p.p., comma 3"; Cass. pen., Sez. V, 26 marzo 2010, n. 21878, cit.; Cass. pen., Sez. IV, 28 settembre 2006, n. 35860, cit.

afferma che gli elementi probatori tratti da un colloquio intercettato, quando si risolvano in accuse verso terzi (e non anche *contra se*), costituiscono (giustamente) prove indiziarie e, come tali, soggiacciono ai criteri di valutazione di cui all'art. 192, comma 2, c.p.p.[88].

In definitiva, può dirsi che l'espressione "circostanza indiziante" impiegata dalla giurisprudenza onde descrivere il regime di utilizzabilità del materiale autoaccusatorio captato sia assolutamente fuorviante. Essa, più correttamente, dovrebbe essere interpretata in base a una lettura sistematica dello strumento captativo nel contesto dei mezzi di ricerca della prova. Se, come qui sostenuto, l'intercettazione si caratterizza per il suo "ibridismo probatorio" – inteso come la commistione di prova critica e prova dichiarativa – non è irragionevole affermare che a fronte di una *contra se declaratio* l'elemento dichiarativo prevalga su quello indiziante, con conseguente inoperatività dell'art. 192, comma 2, c.p.p. Sicché, il giudice, in conseguenza dell'adozione della tesi che postula la piena utilizzabilità delle dichiarazioni autoaccusatorie, deve valutare queste ultime alla stregua del principio del libero convincimento, senza essere vincolato dai parametri della precisione, gravità e concordanza.

4. Sintesi

La risposta al quesito posto in apertura – quale sia, cioè, la sorte delle dichiarazioni *contra se* captate nel corso di un'intercettazione telefonica – muta a seconda del punto di osservazione adottato dall'interprete.

L'impostazione dottrinale dominante, nel teorizzarne la piena valenza probatoria, esclude qualsiasi profilo di frizione con la garanzia del diritto al silenzio, facendo leva su una nozione "esternalizzante" di autodeterminazione. La libertà di scelta dell'indagato deve essere tutelata allorquando si instauri un contatto dialettico e diretto con l'autorità procedente: solo in questi casi, infatti, vi è il rischio che vengano esercitate nei confronti di quest'ultimo pressioni fisiche o psicologiche, tali da alterare il suo percorso volitivo. Lo "stimolo" proveniente *ab extra* costituisce, dunque, il requisito di operatività del diritto al silenzio e a non autoincriminarsi. È in questo senso – come osservato – che si colloca la più nota (e autorevole) definizione del concetto di "libertà morale" (bene oggetto di tutela del *nemo tenetur se detegere*)[89]: "facoltà della persona fonte di prova di determinarsi liberamente rispetto agli stimoli"[90].

Da un'angolazione interpretativa differente, una parte della letteratura accoglie una concezione "interiorizzante" del principio di autodeterminazione: ogni apporto probatorio offerto dall'indagato durante il procedimento dovrebbe essere frutto di una scelta pienamente consapevole. In caso contrario – come accade, ad esempio, nelle intercettazioni – la sua libertà morale non può dirsi realmente salvaguardata.

Il diritto giurisprudenziale, lo si è visto, ha aderito alla prima esegesi.

Le conseguenze di una simile impostazione, però, non sono state colte a pieno: come si è cercato di dimostrare, una volta ammessa la legittima spendibilità processuale del risultato della "captazione confessoria", il giudice potrà apprezzarne il contenuto alla stregua del canone del libero convincimento, non trovando applicazione i limiti legislativi previsti all'art. 192, comma 2, c.p.p.

88. Cass. pen., Sez. V, 17 luglio 2015, n. 4572, in "OneLegale", in cui si afferma che "le accuse verso terzi tratte dal contenuto di un colloquio intercettato […] hanno valenza di indizio, e come tali richiedono una corretta valutazione da parte del giudice; su un piano generale, infatti, richiamando anche nella materia de qua le nozioni di cui all'art. 192 c.p.p., comma 2, è stato segnalato che gli indizi raccolti nel corso delle intercettazioni telefoniche possono costituire fonte diretta di prova della colpevolezza dell'imputato e non devono necessariamente trovare riscontro in altri elementi esterni, qualora siano: a) gravi, cioè consistenti e resistenti alle obiezioni e quindi attendibili e convincenti; b) precisi e non equivoci, cioè non generici e non suscettibili di diversa interpretazione altrettanto verosimile; c) concordanti, cioè non contrastanti tra loro e, più ancora, con altri dati o elementi certi"; Cass. pen., Sez. VI, 4 novembre 2011, n. 3882, cit.; Cass. pen., Sez. IV, 17 ottobre 1991, n. 1035, in CED 189043.

89. Grevi 2009, p. 28.

90. Vassalli 1997, p. 306 s.

Riferimenti bibliografici

T. Alesci (2017), *Il corpo umano fonte di prova*, CEDAM, 2017

E. Amodio (1974), *Diritto al silenzio o dovere di collaborazione? A proposito dell'interrogatorio dell'imputato in un libro recente*, in "Rivista di diritto processuale", 1974

R. Angeletti (2021), *Il processo indiziario. Indizio, sospetto e congettura al vaglio della giurisprudenza di legittimità*, Giappichelli, 2021

A. Balsamo (2018), *The Content of Fundamental Rights*, in R.E. Kostoris (ed.), "Handbook of European Criminal Procedure", Springer, 2018

G. Bellavista (1961), voce *Confessione (dir. proc. pen.)*, in "Enciclopedia del diritto", vol. VIII, Giuffrè, 1961

M. Bontempelli (2018), *Il captatore informatico in attesa della riforma*, in "Diritto penale contemporaneo", 2018

C. Bonzano (2017), *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Giuffrè, 2017

S. Buzzelli (1990), *Il contributo dell'imputato alla ricostruzione del fatto*, in "Rivista italiana di diritto e procedura penale", 1990, n. 3

A. Camon (2014), *La disciplina delle indagini genetiche*, in "Cassazione penale", 2014, n. 4

F. Caprioli (2017), *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in "Revista Brasileira de Direito Processual Penal", vol. 3, 2017, n. 2

N. Carulli (1985), *La difesa dell'imputato*, Jovene, 1985

E.M. Catalano (2011), *Diritto al silenzio, right not to be questioned e tutela dalla autoincriminazione. Note storico comparative*, in "Cassazione penale", 2011, n. 11

E.M. Catalano (2008), voce *Prova (canoni di valutazione della)*, in "Digesto delle discipline penalistiche", Utet, 2008

V. Cavallari (1968), *La capacità dell'imputato*, Giuffrè, 1968

C. Cesari (2019), *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in "Revista Brasileira de Direito Processual Penal", vol. 5, 2019, n. 3

A. Chelo (2025), *La tutela della libertà morale nella formazione della prova penale*, CEDAM, 2025

A. Chelo (2022), *Tutela della libertà morale e captatore informatico: è davvero tutto concesso a soddisfazione delle esigenze investigative?*, in "Diritto penale e processo", 2022, n. 7

M. Chiavario (2002), *Contraddittorio e "ius tacendi": troppo coraggio o troppa prudenza nell'attuazione di una riforma costituzionale a rime non sempre obbligate?*, in "Legislazione penale", 2002

M. Chiavario (1982), *Processo penale e garanzie della persona*, vol. II, Giuffrè, 1982

C. Conti (2003), *L'imputato nel procedimento connesso. Diritto al silenzio e obbligo di verità*, CEDAM, 2003

F. Cordero (2012), *Procedura penale*, Giuffrè, 2012

F. Cordero (1987), *Procedura penale*, Giuffrè, 1987

P. Corso (1999), *Diritto al silenzio: garanzia da difendere o ingombro processuale da rimuovere?*, in "Indice penale", 1999, n. 3

M.L. Di Bitonto (2008), *Il diritto al silenzio dell'imputato*, in "Giurisprudenza di merito", 2008, n. 7-8

O. Dominioni (1989), *sub Art. 66-68*, in E. Amodio, O. Dominioni (a cura di), "Commentario del nuovo codice di procedura penale", Giuffrè, 1989

O. Dominioni (1985), *Le parti nel processo penale*, Giuffrè, 1985

F. Falato (2022), *L'evoluzione della dogmatica processuale nella fisionomia "europea" del diritto al silenzio. Questioni esegetiche da risolvere*, in "Archivio penale web", 2022, n. 1

C. Fanuele (2009), *Dati genetici e procedimento penale*, CEDAM, 2009

E. Fassone (1989), *Primi appunti sulla valutazione della prova nel nuovo processo penale*, in "Questione giustizia", 1989

P. Felicioni (2007), *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, 2007

P. Ferrua (2020), *Teorie della prova: dialogo con Franco Cordero*, in "Discrimen", dicembre 2020

P. Ferrua (2018), *La prova nel processo penale*, in "Revista Brasileira de Direito Processual Penal", vol. 4, 2018, n. 1

P. Ferrua (2005), *La prova nel dibattimento penale*, Giappichelli, 2005

P. Ferrua (1989), voce *Difesa (diritto di)*, in "Digesto delle discipline penalistiche", vol. III, Utet, 1989

L. Filippi (2021), *Ma davvero si può ricorrere a manovre fraudolente per intercettare col virus trojan?*, in "PenaleDP", 9 febbraio 2021

L. Filippi (1997), *L'intercettazione di comunicazioni*, Giuffrè, 1997

E. Florian (1924), *Delle prove penali*, vol. II, Casa editrice Francesco Vallardi, 1924

G. Foschini (1961), *Sistema del diritto processuale penale*, vol. II, Giuffrè, 1961

C. Gabrielli (2012), *Il prelievo coattivo di campioni biologici nel sistema penale*, Giappichelli, 2012

N. Galantini (2024), *Il diritto al silenzio: da Boomer a Generazione Alpha*, in "Processo penale e giustizia", 2024, n. 5

N. Galantini (1992), *L'inutilizzabilità della prova nel processo penale*, CEDAM, 1992

V. Gianturco (1958), *La prova indiziaria*, Giuffrè, 1958

A. Giarda (2007), *Dichiarazioni autoaccusatorie "intercettate" in conversazioni e comunicazioni*, in "Corriere del merito", 2007, n. 11

A. Giarda (1980), *Persistendo 'l reo nella negativa*, Giuffrè, 1980

M.S. Green (1999), *The Privilege's Last Stand: the Privilege Against Self-Incrimination and the Right to Rebel Against the State*, in "Brooklyn Law Review", vol. 65, 1999, n. 3

K. Greenawal (1974), *Perspectives on the Right to Silence*, in R. Hood (ed.), "Crime Criminology and Public Policy", Free Press, 1974

V. Grevi (2009), *Le intercettazioni al crocevia tra efficienza del processo e garanzie dei diritti*, in Aa.Vv., "Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti", Giuffrè, 2009

V. Grevi (2000), *Alla ricerca di un processo penale «giusto». Itinerari e prospettive*, Giuffrè, 2000

V. Grevi (1998), *Diritto al silenzio dell'imputato sul fatto proprio e sul fatto altrui*, in "Rivista italiana di diritto e procedura penale", 1998

V. Grevi (1973), *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in "Giurisprudenza costituzionale", 1973, n. 1

V. Grevi (1972), *«Nemo tenetur se detegere». Interrogatorio e diritto al silenzio nel processo penale italiano*, Giuffrè, 1972

V. Grevi (1971), *Intercettazioni telefoniche e principi costituzionali*, in "Rivista italiana di diritto e procedura penale", 1971

F.M. Iacoviello (1997), *La motivazione della sentenza penale e il suo controllo in Cassazione*, Giuffrè, 1997

G. Illuminati (2013), *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in Aa.Vv., "Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi ad un anno dalla sua scomparsa", CEDAM, 2013

G. Illuminati (2012), *Nemo tenetur se detegere: il pilastro dell'autodifesa nel pensiero di Vittorio Grevi*, in "Rivista di diritto processuale", 2012, n. 5

G. Illuminati (1999), *I principi generali del sistema processuale penale italiano*, in "Politica del diritto", 1999, n. 2

G. Illuminati (1993), *In difesa del diritto al silenzio*, in "Indice penale", 1993

G. Illuminati (1983), *La disciplina processuale delle intercettazioni*, Giuffrè, 1983

G. Illuminati (1979), *La presunzione d'innocenza dell'imputato*, Zanichelli, 1979

J. Jackson (2009), *Re-Conceptualizing the Right of Silence as an Effective Fair Trial Standard*, in "International and Comparative Law Quarterly", vol. 58, 2009, n. 4

G. Lozzi (2006), *Lezioni di procedura penale*, Giappichelli, 2006

L. Lupària (2006), *La confessione dell'imputato nel sistema processuale penale*, Giuffrè, 2006

G. Montalbano (1958), *La confessione nel diritto vigente*, Jovene, 1958

A. Macchia (1989), voce *Confessione (dir. proc. pen.)*, in "Digesto delle discipline penalistiche", vol. III, Utet, 1989

A. Mangiaracina (2021), *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici … e non solo*, in "Processo penale e giustizia", 2021, n. 4

V. Manzini (1982), *Trattato di diritto penale italiano*, vol. V, in G.D. Pisapia (a cura di), "Delitti contro l'amministrazione della giustizia", Utet, 1982

L. Marafioti (2000), *Scelte autodifensive dell'indagato e diritto al silenzio*, Giappichelli, 2000

P. Marchetti (1994), *Testis contra se. L'imputato come fonte di prova nel processo penale d'età moderna*, Giuffrè, 1994

O. Mazza (2014), *Presunzione d'innocenza e diritto di difesa*, in "Diritto penale e processo", 2014, n. 12

O. Mazza (2004), *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Giuffrè, 2004

A. Melchionda (1997), voce *Prova in generale (dir. proc. pen.)*, in "Enciclopedia del diritto", Giuffrè, 1997

M. Miraglia (2023), *Il "Trojan (non) di Stato". Una disciplina da completare*, in "Processo penale e giustizia", 2023, n. 5

P. Moscarini (2014), *Princìpi delle prove penali*, Giappichelli, 2014

P. Moscarini (2010), voce *Silenzio dell'imputato (diritto al)*, in "Enciclopedia del diritto", Annali, vol. III, Giuffrè, 2010

P. Moscarini (2006), *Il diritto al silenzio dell'imputato sul fatto proprio secondo la Corte di Strasburgo e nell'esperienza italiana*, in "Rivista italiana di diritto e procedura penale", 2006, n. 2

F. Munoz Conde (2009), *Dal divieto di autoincriminazione al diritto processuale penale del nemico*, in "Archivio penale", 2009, n. 2

M. Nobili (1989), *La nuova procedura penale. Lezione agli studenti*, Clueb, 1989

L. Paladin (1965), *Autoincriminazioni e diritto di difesa*, in "Giurisprudenza costituzionale", 1965

G. Pansini (2018), *Le prove deboli nel processo penale italiano*, Giappichelli, 2018

L. Parlato (2020), Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale, in "Processo penale e giustizia", 2020, n. 2

V. Patanè (2024), *Nemo tenetur se detegere: coordinate europee e parametri costituzionali del diritto a non collaborare dell'imputato*, in "Cassazione penale", 2024, n. 6

V. Patanè (2006), *Il diritto al silenzio dell'imputato*, Giappichelli, 2006

S. Rodotà (2012), *Il diritto di avere diritti*, Laterza, 2012

M. Scaparone (1980), *Evoluzione e involuzione del diritto di difesa*, Giuffrè, 1980

S. Signorato (2018), *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018

L. Scomparin (2002), *La tutela del testimone nel processo penale*, CEDAM, 2002

L. Tassinari (2012), *Nemo tenetur se detegere. La libertà dalle autoincriminazioni nella struttura del reato*, Bononia University Press, 2012

P. Tonini (2002), *Il diritto al silenzio tra giusto processo e disciplina di attuazione*, in "Cassazione penale", 2002, n. 2

P. Tonini (2000), *La prova penale*, Giappichelli, 2000

P. Tonini, C. Conti (2024), *Manuale di procedura penale*, Giuffrè, 2024

P. Tonini, C. Conti (2014), *Il diritto delle prove penali*, Giuffrè, 2014

M. Torre (2017), *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017

G. Ubertis (2008), voce *Giusto processo (dir. proc. pen.)*, in "Enciclopedia del diritto", Annali, vol. II, Giuffrè, 2008

G. Ubertis (2000), *Principi di procedura penale europea*, Giuffrè, 2000

G. Ubertis (1995), *La prova penale. Profili giuridici ed epistemologici*, Utet, 1995

G. Vassalli (1997), *Scritti giuridici. Il processo e le libertà*, vol. III, Giuffrè, 1997

F. Zacché (2008), *Gli effetti della giurisprudenza europea in tema di privilegio contro le autoincriminazioni e diritto al silenzio*, in A. Balsamo, R.E. Kostoris (a cura di), "Giurisprudenza europea e processo penale", Giappichelli, 2008

Sezione monografica

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? - Part II

a cura di

Elda Brogi

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0228 • articolo sottoposto a peer review • pubblicato in anteprima il 2 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Roberta Carlini

Market power and opinion power. Assessing the risks for media pluralism and editorial independence deriving from ownership's concentration

In premise, we explain why media ownership concentration still matters in the digital age, summarising the relevant literature and the evolution of the European policy debate leading to Article 22 EMFA (assessment of media market concentrations, the so-called "Media plurality test"). We will then expose the rationale for a holistic perspective, which goes beyond the competition law to take into account the broader impact of media ownership concentration on the formation of public opinion, diversity of offer and editorial independence (supply side), as well as the plurality of exposure (demand side). Then we describe the keywords and key indicators of the "Media plurality test", using the conceptual tools and result of the Media Pluralism Monitor research project to critically analyse its scope and criteria; to investigate potential issues; and to discuss the relationship between ownership's concentrations and editorial independence. Finally, we highlight the main challenges ahead.

Ownership – Concentration – Pluralism – Editorial independence – Market power – Media plurality test – EMFA

Potere di mercato e controllo dell'opinione pubblica. La valutazione dei rischi per il pluralismo e l'indipendenza editoriale derivanti dalla concentrazione proprietaria

In premessa, spieghiamo perché la concentrazione della proprietà dei media conta ancora, anche nell'era digitale, riassumendo la letteratura scientifica e l'evoluzione del dibattito politico in Europa che ha portato all'articolo 22 dell'EMFA (valutazione delle concentrazioni del mercato dei media, il cosiddetto "Media plurality test"). Di seguito argomentiamo le ragioni di un approccio olistico, che vada oltre la normativa a tutela della concorrenza per valutare il più ampio impatto della concentrazione della proprietà dei media sulla formazione dell'opinione pubblica, sulla diversità dell'offerta informativa e sulla indipendenza editoriale (lato offerta), nonché sulla diversità nell'esposizione e accesso ai media (lato domanda). Poi si introducono le parole-chiave e gli indicatori del "Media plurality test", utilizzando gli strumenti concettuali e i risultati del progetto di ricerca Media Pluralism Monitor per analizzarne criticamente la portata e i criteri, per indagare i potenziali problemi e per discutere la relazione tra le concentrazioni di proprietà e l'indipendenza editoriale. Infine, si evidenziano le principali sfide da affrontare.

Proprietà – Concentrazione – Pluralismo – Indipendenza editoriale – Potere di mercato – Media plurality test – EMFA

The Author is Part-time Assistant Professor at the Centre for Media Pluralism and Media Freedom, European University Institute

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: 1. Why media ownership concentration matters. – 2. The policy debate in the EU leading to Art. 22 EMFA. – 3. The Media plurality test: keywords and key indicators. – 4. What Art. 22 (and EMFA) do not do. – 5. Scope and criteria of the Media plurality test. – 6. The main challenges ahead. – 7. Conclusions.

1. Why media ownership concentration matters

In the digital era, all the news is just one click away, one could say echoeing Google's mantra[1]. Regardless of how concentrated the media market may be, it is always possible to find a diverse sources of information, as long as the internet is open. On the supply side, lower production and distribution costs have reduced barriers to access, enabling also non-professionals and users to become news sources. On the demand side, news content can be accessed from anywhere in the world, limited only by language differences and technical barriers.

However, there are several reasons to argue that the digital revolution has not resolved or diminished the issue of market power within media systems, highlighting the ongoing need to address it. The specific rules and procedures designed to tackle this problem must be revised and adapted to align with the digital environment and the new dominant players within it[2].

The reasons for arguing that concentration of ownership still matters in the digital era are empirical, theoretical and normative.

From an empirical perspective, indicators demonstrate that media market concentration has increased globally in the digital age[3]. On the production side, the internet's abundance of opportunities and diverse voices has not led to the emergence of new, robust media entities that effectively challenge the legacy media conglomerates in terms of content creation. On the distribution side, new players have emerged with significant and growing market power, acting as intermediaries between the audiences and the sale of their attention to advertisers. The role of online platforms has disrupted the traditional business model of commercial media, jeopardizing both their revenue streams from sales and advertising[4]. Consequently,

1. Point 4 of the Google's approach to competition.
2. Moore–Tambini 2018, Montjoye–Schweitzer–Crémer 2019; Stigler Committee on Digital Platforms 2019; Stigler Media Subcommittee 2019; Furman–Coyle–Fletcher et al. 2019; Prat 2020; Nielsen–Ganter 2022.
3. Noam 2016; CMPF 2024, pp. 70-75.
4. Anderson–Julien 2015; Parcu 2019; OECD 2021.

this trend has prompted traditional media to concentrate and consolidate further; the rationale for large-scale operations, previously justified by fixed costs and the technological characteristics, is increasingly framed as a necessary strategy to compete in the digital landscape and ensure the sustainability of the media industry[5].

From a theoretical perspective, equating media market plurality with media pluralism is challenged by two main arguments. The first argument focuses on the limits of the liberal approach based on the "marketplace of ideas", which posits that free individual choice in competitive markets is both necessary and sufficient conditions for achieving media pluralism. Critics of this approach argue that dispersal of ownership in the market and media pluralism do not always align – diversity of offer can be guaranteed even in a single-media system, and conversely competitive media outlets can offer a uniformed content; and that, more generally, this framework has proven as "inadequate for conceptualizing the complex nature of media pluralism as a broader public interest value"[6]. The second argument delves in the difference between market power and opinion power, arguing that the threat to pluralism does not stem solely from the ownership structure, but rather from how the owners manage the media, and the potential interference of their behaviour with the democratic process: in this perspective, "ownership really isn't the problem, but is a proxy for other concerns"[7]. The consequence is a more holistic concept of media pluralism, which distinguishes the European debate from the US approach: "In the US, debates over pluralism tend to focus on ownership, with an occasional reference to broadcast policies such as the fairness doctrine (…). The European debate, however, tended to take a more Habermasian public sphere approach, and to focus on the role of the media in maintaining and limiting participation in the public sphere". As a consequence, "concentration law and ownership limits emerged much later in Europe than the US, but have had limited effect in solving pluralism concerns"[8].

It must be underlined that this holistic approach does not cancel the need to look at media ownership structure and address the risks related to media market concentration. In this approach, media ownership concentration still matters, even though it must be considered and evaluated together with other dimensions of pluralism. Adopting this perspective, the Media Pluralism Monitor, implemented by the Centre for Media Pluralism and Media Freedom since 2014, evaluates the concentration of media ownership as one of the 20 indicators to assess the risks for media pluralism in the EU and candidate countries; in 2020, following a reconceptualization of the tool to address the new characteristics and structure of the markets in the digital environment, another indicator of concentration has been added, measuring the market power of other actors that, even though are not media strictu sensu, have an essential function in intermediating distribution of and access to the media content: digital intermediaries such as search engines, social media, automatic aggregators and artificial intelligence models. Adding the indicator of concentration in the digital markets to the "traditional" indicators of media ownership concentration, the Media Pluralism Monitor aimed to include in its methodology the assessment of the risks for media pluralism deriving from the structural features of the digital markets, both for their winner-take-all dynamic and for their disruptive effects on the economic sustainability of the media[9].

Finally, the normative approach adds arguments to address the issue of market power in the media sector. As seen above, it is possible that even in a very concentrated market, with a total lack of external pluralism, there is a vital and effective internal pluralism, with a rich offer of diverse content by the dominant media outlet. But, let alone the difficulties of measuring the diversity of content, there are no guarantees on the fact that this situation would not change, in case of a change of ownership, or a change of editorial line. As argued

5. Carlini–Parcu 2024.
6. Karppinen 2013, p. 8.
7. Picard–Dal Zotto 2016.
8. Valcke–Süksd–Picard 2016, pp. 3-4.
9. Parcu 2019.

by C.E. Baker in his seminal work, dispersal of media ownership should be considered as an end in itself, a "pure process" value, as a democratic safeguard[10]. The digital transformation did not solve the problem[11], adding new and different sources of concern, in terms of exposure to diversity and agenda control[12]. These sources of concern seem to be confirmed by recent developments in the political and media environment after the US presidential elections in 2024, with the political alignment of the owners of the biggest tech companies, and the editorial choice in media that they control[13].

2. The policy debate in the EU leading to Art. 22 EMFA

In the European Union, the first attempt to address excessive concentration of media ownership dates back to 1992, with the European Parliament Resolution on media concentration and diversity of opinions[14], followed by the Green Paper of the European Commission[15]; but the European Commission's initiative with a proposal for a directive in 1996-7 fell through the opposition of political parties and industry stakeholders[16]. In 2007, another phase began, substantially based on "monitoring and soft governance" in the field of media pluralism[17]. This phase was characterized by a "three-step approach" and a "risk-based approach"; a relevant evolution occurred in 2020, with the European Democracy Action Plan and the State of the Rule of Law first report, envisaging media pluralism assessment as a part of the rule of law mechanism[18]; but in both cases, no specific and binding provisions were related to the rules on media ownership concentration at the EU level. At the national level, the legal framework on media ownership concentration is diversified and fragmented. As highlighted by the mapping of the Study on media plurality and diversity online[19], 14 Member States have special rules to evaluate media mergers, but with different methods and criteria (not always the protection of media pluralism is considered among the criteria). The study also highlights that "the problematic issue remains that the relevant rules rarely provide explanations of what is meant by media pluralism and the public/general interest considerations, which are used as bases for justifying interventions and that give additional power to one authority over another"[20]. The fragmentation of national rules is also problematic for their potential use to pursue goals and protect interests other than media pluralism; and for the obstacles that a fragmented legal framework poses to the common media market.

The negative impact of the fragmentation of the Member States' rules and procedures on media concentrations on the functioning of the internal market provides the rationale and the legal base for Article 22 EMFA, as explained in Recital 63: "In order to reduce obstacles which hinder media service providers' ability to operate in the internal market, it is important that this Regulation set out a common framework for assessing media market concentrations across the Union." Thus, the EU's first attempt to pass "from rhetoric to

10. Baker 2007, pp. 18-19. Using Baker's approach, and comparing approaches and instruments in Europe and US, Just 2009 advocates for "a return to the normative principle as primary guiding element of communication policy making. The emphasis should be put on a wide dispersal of independent media ownership as a guarantor of the proper functioning of the public sphere as the ultimate and of communication policy".
11. Baker 2007, pp. 97-123; Doyle 2016.
12. Schlosberg 2017.
13. Baron 2025; Mymbs Nice 2025; Burman 2025.
14. Available on Publication Office website.
15. Dossier COM(92)480 vol. 1992/0218.
16. Fanta 2014.
17. Karppinen 2013, p. 144.
18. Brogi–Da Costa Leite Borges–Carlini et al. 2023, pp. 21-24.
19. European Commission 2022.
20. *Ivi*, p. 219.

regulation" on media concentration[21] is a sort of soft harmonization, as it needs national rules and procedures to introduce in the Member States' legal frameworks the "Media plurality test". As pointed out by Manganelli and Mariniello[22], the starting assumption is that the competition law is not sufficient to guarantee media pluralism and that in the evaluation of concentrations that could impact media pluralism and editorial independence a separate assessment is needed, to take into consideration other potentially harmful effects of the merger, related to the formation of the public opinion, the democratic process and ultimately to the fundamental right to information stated by Article 11 of the Charter of Fundamental Right of the European Union on Freedom of expression and information, and specified by Article 3 of the EMFA as "the right of recipients of media services to have access to a plurality of editorially independent media content".

3. The Media plurality test: keywords and key indicators

The notion of media pluralism enshrined in Art. 3 and Art. 22 of the EMFA, although aimed at protecting the well-functioning of the internal market, goes beyond a mere economic perspective and embeds a holistic view of pluralism. In this perspective, it should not be sufficient to consider the concentration or dispersal of media ownership, on the supply side, but also the information habits and exposure to diversity should be investigated and evaluated, on the consumption side; on both sides, taking into consideration the digital environment of production, distribution and consumption of the news.

Moreover, Art. 22(1) asks to consider jointly the impact of concentrations on media pluralism and editorial independence. The intertwining between the two dimensions is further demonstrated by the fact that, together with its proposal for a European Media Freedom Act, the European Commission issued its Recommendation on internal safeguards for editorial independence and ownership transparency in the media sector[23].

Finally, any Media plurality test on a merger should consider what would be the impact on media pluralism and editorial independence in the absence of the merger itself: e.g., if the survival of the media would be at risk without the merger, for lack of economic sustainability. Also in this case, the criteria for an assessment in the perspective of media pluralism do not necessarily coincide with the criteria to evaluate the defensive mergers set by the competition law.

Before analysing the criteria set by Art. 22(2) to conduct the Media plurality test, is worth reading its keywords – media concentration, online environment, editorial independence and media economic sustainability – in the light of the results of the correspondent indicators of the Media Pluralism Monitor (MPM). The indicator of concentration of the media providers has always been the one at the highest level of risk in Europe since the beginning of the measurement and without exception across the European countries. Since 2020, an indicator of the concentration of online platforms has been added, showing a similar, if not higher, level of risk. In parallel, the results of the MPM signal an increase in the risk level for the indicator on Editorial independence from commercial and owners' influence, whereas the indicator on economic sustainability of the media ("Media viability") reflects the growing difficulties in the media financing, with some signals of resilience only in the last year (see Fig. 1).

In other words, the MPM results confirm the need to address the issue of media ownership concentration and to frame it into the digital environment of the media; and they highlight the deteriorating economic conditions of the media and the risks for editorial independence. All the dimensions of pluralism that Article 22 aims to evaluate and protect are at medium or high risk in the average of the European countries. The question is: is it possible to pursue all the objectives – tackling concentration, sustaining media and protecting editorial independence – with a single tool, the Media plurality test? To answer this question, it is worth first clarifying what Art.

21. Kerševan 2024.

22. Manganelli–Mariniello 2024.

23. European Commission, C(2022) 6536 Commission recommendations on internal safeguards for editorial independence and ownership transparency in the media sector, 16 September 2022.

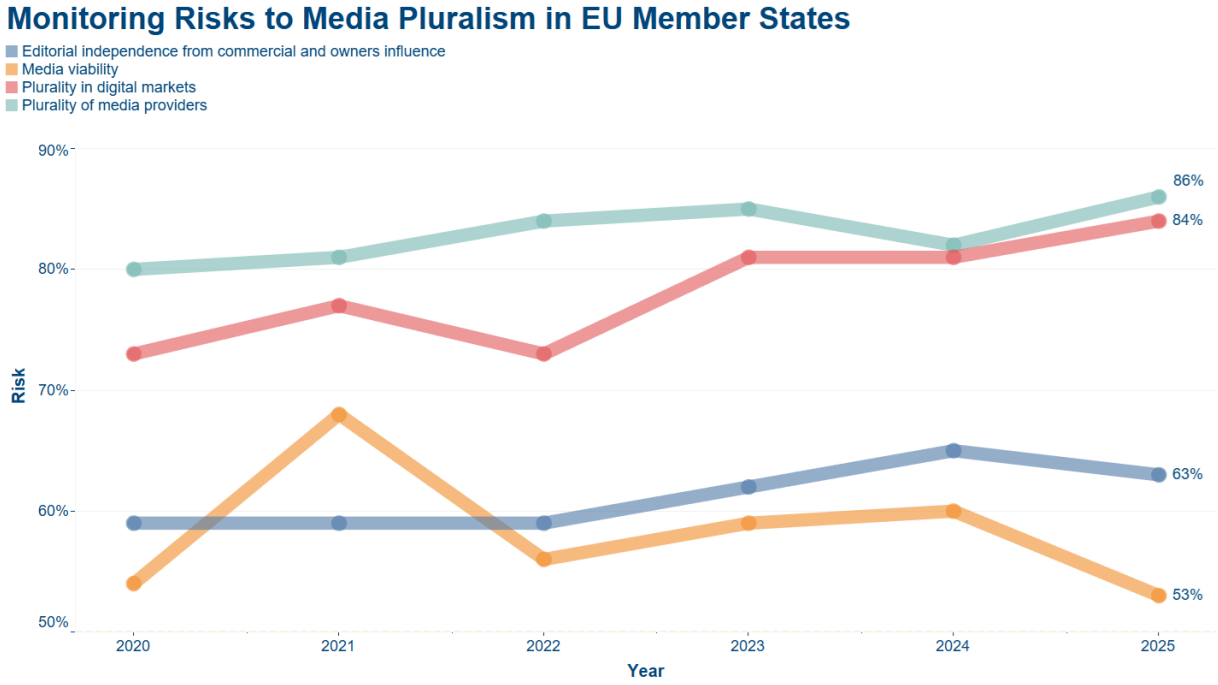

Fig. 1 — *Economic threats to media pluralism – The results of Media Pluralism Monitor. Source: Media Pluralism Monitor*

22 does not do; then analysing its scope and the criteria set to assess the impact of a media market concentration on media pluralism and editorial independence.

4. What Art. 22 (and EMFA) do not do

Art. 22 does not address the situation in which a high concentration of media ownership is already established because it only intervenes in cases of mergers that might impact media pluralism and editorial independence. "Existing high levels of concentration that could significantly impact media pluralism and editorial independence, and even new concentrations arising from the market growth of a player, or closures or downsizing of other players, are not caught by the provision"[24]; nor are they caught by other tools of the new EU regulation – except for the monitoring exercise introduced in the final provisions, which includes "the level of media concentration" (Art. 26(3) EMFA). Nonetheless, the level of concentration pre-existing the merger would be an element to evaluate it, and the monitoring exercise envisaged in Art. 26 can be a relevant help, particularly for countries in which the information on the media market is not transparent or insufficient.

Moreover, neither Art. 22 nor other provisions in the EMFA directly address the issue of the economic crisis of the media and the eventual need for public support for a good that is at risk of under-financing by the market. In Section 6 of the Act the goal of "Transparent and fair allocation of economic resources" is named in the title, but only some pre-conditions for a fair allocation of resources are addressed, namely audience measurement (Art. 24) and transparent and non-discretionary rules for state advertising (Art. 25). Public support to the media, at national or at EU level, is out of the scope of the Act. The issue of economic sustainability of the media service providers only enters into play as one of the criteria to evaluate the impact of a concentration.

5. Scope and criteria of the Media plurality test

The "media market concentrations" that shall be submitted to the Media plurality test are defined in Art. 2(15) of EMFA: "a concentration as defined in

24. Carlini–Parcu 2024.

Art. 3 of Regulation (EC) No 139/2004 involving at least one media service provider or one provider of an online platform providing access to media content". Thus, a concentration, as defined under the EC merger regulation, falls under the scope of Art. 22 depending on the actors involved. This is obviously the case in which a media service provider is involved. Interestingly, this is also the case in which other actors are involved, which are outside the original perimeter of traditional media, defined as "online platforms providing access to media content". The inclusion of the latter in the scope of Art. 22 was not contemplated in the Commission's proposal and has been added during the legislative process. The phrasing can give room to some doubts of interpretation, also considering that the definition does not coincide with the phrasing of the Digital Services Acts and the same Art. 18 EMFA (regulating the obligations of very large online platforms concerning the content of media service providers): must the use of the platform to access media content be proved, or shall it be considered among the structural features of social media, search engines, automatic aggregators, and AI assistants? Nonetheless, it seems clear that the EU legislator with this provision asks to take into consideration the role of the digital intermediaries in the media environment, following a growing corpus of literature that reconceptualizes the definition of the media in the digital era[25]. According to the definition of Art. 2(15), a merger involving a platform providing access to media, e.g., between two social media, or a social media and a news aggregator, or between a search engine and an AI company, might be cleared under Art. 22 under the European Union law, to assess its impact on media pluralism and editorial independence. Even though a merger may seem a remote hypothesis, and even though the platform dependency of the media is not directly exercised through ownership control, the provision marks a relevant step forward to the inclusion of the digital intermediaries in the media regulatory framework.

The need to take into account the online environment, other than in the scope of application of Art. 22, is listed among the criteria of the Media plurality test in Art. 22(2). As noticed by Manganelli and Mariniello[26], these criteria outline general principles that the European Commission must specify in the upcoming guidelines, not only to detail their provisions but also to define their reciprocal relationship.

They are listed in five points, as follows:

a) the expected impact of the media market concentration on media pluralism, including its effects on the formation of public opinion and on the diversity of media services and the media offering on the market, taking into account the online environment and the parties' interests in, links to or activities in other media or non-media businesses;
b) the safeguards for editorial independence, including the measures taken by media service providers with a view to guaranteeing the independence of editorial decisions;
c) whether, in the absence of the media market concentration, the parties involved in the media market concentration would remain economically sustainable, and whether there are any possible alternatives to ensure their economic sustainability;
d) where relevant, the findings of the Commission's annual rule of law report concerning media pluralism and media freedom; and
e) where applicable, the commitments that any of the parties involved in the media market concentration might offer to safeguard media pluralism and editorial independence.

Point a) is very dense and groups different factors, mixing elements on the supply and demand side. First, it clarifies that the assessment should consider the impact of the merger on the control of

25. The Study on media plurality and diversity online, commissioned by the European Commission, recaps the evolution of the definition of media in policy documents and in the scientific debate; alongside with the "Media actors", and the "Other media actors and public watchdogs reporting on matters of public interest", it defines "Other actors, intermediary and auxiliary services, in the media ecosystem" as "intermediary or auxiliary services which contribute to the functioning or accessing of a media, but do not or should not exercise editorial control, and therefore have limited or no editorial responsibility, may not be considered to be media" (European Commission 2022, p. 17).

26. Manganelli–Mariniello 2022.

public opinion, and therefore it should go beyond the mere economic evaluation. Second, it asks to evaluate the impact of the merger on the diversity of media offerings and media services. Third, to evaluate both (impact on public opinion and on media diversity) it asks to consider the online environment: a vague definition that seems to call for an evaluation not only for the evaluation of the digital offer of the media but also of the consumption habits and the information diet of the interested audience. In the UK system, where a separate assessment for media mergers called "public interest test" is required, Ofcom bases its evaluation on a periodical survey of media consumption habits; and a debate on the reconceptualization and fine-tuning of the test in the digital environment of the news has been carried on[27]. It is worth noting that not only in the European Union countries this kind of official survey is not frequent; but also that, if they shall base the implementation of Art. 22 of EMFA, it would be necessary for them to have the same methodology and scope, to have a harmonized Media plurality test across all the Member States. Finally, in point a) another element on the supply side is added, and it is the evaluation of the nature of the entities involved, in particular of their links or interests "in other media or non-media businesses." The latter element seems to reflect a growing concern for the mixed interests in media ownership, which can be detrimental to the editorial independence of the media outlets from their owners' interests when they are other than the success of the same media undertaking. According to the results of the Media Pluralism Monitor, "It is common that media owners have significant interests in other sectors, such as real estate, construction, banking, telecommunications, and gambling. Only four countries (Denmark, Finland, Sweden, and the Netherlands) reported that their market leaders were only investing in sectors that were connected to the media. Having interests in other sectors constitutes a risk for media pluralism, as media outlets might provide biased coverage of their owners' other businesses; moreover, if those businesses are dependent on public contracts or might be subject to strict regulation, the economic interests can easily be translated into political favours that can undermine the media's watchdog function"[28].

Point b) clarifies the tight intertwining between the two cores of the Media plurality test: media pluralism and editorial independence. The Media plurality test may lead to a negative opinion even in cases in which pluralism is not menaced, but editorial independence is reduced. Here, editorial independence is understood as independence of editorial decisions, which is also a duty of media service providers stated by Art. 6 of the EMFA (which drafts a distinction between "established editorial line" and "editorial decisions", protecting the latter from undue interference by the owners).

Point c) introduces the element of economic sustainability of the media. This provision is crucial because media mergers are increasingly justified by the need to avoid the closure of one or all the merging entities. Defensive mergers, contemplated in the competition law, can still be problematic for their impact on media plurality and diversity. The dilemma is presented in many cases and media systems, with different outcomes[29], and it is well visualized in the two opposite opinions recently published concerning the acquisition of RTL by DPG Media in The Netherlands.[30] Art. 22(2, c) addresses this dilemma, asking for the evaluation not only of the actual risk of closure of the media without the merger but also for the evaluation of possible alternatives.

Point d) suggests that the Media plurality test considers the state of media pluralism and media freedom in the country, as assessed by the Commission's annual rule of law report. These findings include not only the media market situation, in terms of transparency and concentration, but also the other dimensions of media pluralism, such as the respect of fundamental rights and freedom of expression, the independence from political pressure, protection of minorities, and other

27. Ofcom 2021; Ofcom 2022.

28. Bleyer-Simon–Da Costa Leite Borges–Brogi et al. 2024, p. 100.

29. Carlini–Parcu 2024.

30. See, on nrc.nl, pro-takeover: *De overname van RTL door DPG is een goed idee* and anti-takeover: *De overname van RTL door DPG is wél een probleem*.

elements of the legal framework and its effectiveness when it comes to media pluralism and media freedom.

Point e) delves into the remedies, asking to evaluate the parties' commitments. Even though the order in which the elements listed above should be interpreted is not specified, it seems reasonable that the national regulatory authority designed by the law to implement the Media plurality test can submit a positive opinion on a merger, even in the lack of one of the elements of point a, b and c, to the parties' commitment to safeguard media pluralism and editorial independence.

As argued in the position paper presented by the Centre for Media Pluralism and Media Freedom during the discussion on the proposal for the EMFA, there is "room for some innovative solutions, which could be specified in the guidelines and in the implementation of the Media Pluralism Test, considering together the principles set by Art. 21 [now 22] and the requirements introduced by Art. 6. In other words: when a merger can be justified by economic reason but still involves a risk for the reduction of the external pluralism, a strengthened set of guarantees in terms of editorial independence, content diversity and internal pluralism can be requested and enforced"[31]. If these guarantees are imposed as a condition for a positive opinion of the merger, they should be considered as structural remedies, not just behavioural ones: a generic commitment of the new media owner to respect independence of editorial decisions of the newsrooms would not be sufficient, whereas structural organizational and internal safeguards, audit and control would be needed.

6. The main challenges ahead

With Article 22, EMFA introduces a relevant and ambitious innovation in the media systems in the European Union. The new Media plurality test presents many challenges, the first obstacle being the fact that Art. 22 requires national rules and procedures to be issued, and the consequent risk of a fragmented and/or not consistent framework across the different countries to evaluate media concentrations in the internal market[32].

The second big challenge of the new anti-concentration framework in the media system is the digital sphere. Although designed in the digital era of the media, with the explicit goal of adapting the old fragmented rules, introduced for analogic media, to the new information scenario, Art. 22 does not directly tackle "the elephant in the room", which is the market dominance of the online platforms and tech companies and the platforms' dependency of the media providers and media users[33]. Though, there are some specific provisions, such as the inclusion of the online platforms in the definition of media market concentrations, and of the online environment among the criteria to conduct the Media plurality test; and a relevant provision on audience measurement (Art. 24), which addresses the big issue of opacity and secrecy in the digital audience measurement systems, whose implementation is a pre-condition of the very possibility to assess the impact of a merger on the "formation of public opinion". Together with the protection set by Art. 18 for the removal of media content on very large online platforms (the so-called "media privilege"), these media-specific rules might interplay with the EU horizontal digital regulation (DSA, DMA, Data Act, AI Act).

While the EMFA and Art. 22 alone cannot address all the challenges of the digital transformation of the media environment, the Media plurality test directly tackles some of the main economic threats to media pluralism and freedom; in particular, linking together the values of media pluralism and editorial independence. In this regard, the main challenge of the Media pluralism test is avoiding a "light", or just formal, interpretation of its criteria, and effectively pursuing the respect of the principles set by the law. This means, for example, that the lack of economic sustainability of the media in the absence of the merger should not just be enunciated as a potential risk, but effectively demonstrated, and other possible alternatives should be explored. Moreover, the possibility of approval of the merger under the condition of safeguards of internal pluralism and editorial independence, if interpreted as calling for structural remedies (as argued

31. CMPF 2023.

32. See Kerševan 2024 for the cases of Croatia and Slovenia, and Sznajder 2024 for Poland.

33. Seipp–Helberger–de Vreese–Ausloos 2024.

above), opens the path to an innovative role of the national authorities – and of the European Board for Media Services, in close cooperation – in exercising toward the private media super visioning competences and powers that were in the past, in some legal frameworks, limited to the public service media. It could be said that, in approving a merger that reduces external pluralism, the regulatory authority recognizes the merged entity as having public value and role which, in turn, comes with some responsibility.

Finally, there is another provision among the criteria of Art. 22 of the EMFA, that was less observed and commented on. It is the request for the rules of the Media plurality test to take into account "the parties' interests in, links in other media or non-media businesses." The rationale for this provision is the augmented potential risks for editorial independence and conflict of interests. Risks that transmigrated from the analogical to the digital environment of the media, as demonstrated by recent cases even in systems in which self-regulatory and professional safeguards proved effective in the past[34].

In his book on Media concentration and democracy, Edwin Baker considers the mixed media/non-media interests as a main threat, at the point that he includes among the policy proposals the following: "any for-profit commercial entity that purchases a media entity must, after the purchase, be primarily in the media business – that is, receive the majority of its revenue from its media business"[35]. In the criteria of Art. 22(2, a), there is clearly a favour for pure media players in the assessment of a merger; in the guidelines that the Commission, assisted by the Board, will publish, as well as in the national laws to implement Art. 22, a simple rule like the one proposed by Baker could be stated. This would go in the direction of simplifying and clarifying the criteria; and also address a worrisome trend toward a new oligarchization of the media, even in countries which were historically immune from this phenomenon.

7. Conclusions

The main aim of Article 22 of EMFA is the harmonization of the fragmented legal framework on media concentration in the single market. As argued above and in other contributions to this monographic section, the main challenges are in the compliance of the Member States' laws, and in their effectiveness. To prevent a new fragmentation with many different versions of the Media pluralism test, it is of the utmost importance that the forthcoming guidelines (issued by the European Commission assisted by the Board) are straightforward and detailed. Moreover, it is important that in the guidelines, as well as in the Board's opinions, a clear interpretation of the scope of Article 22 is shared, regarding: 1) the inclusion in the scope of the Media plurality test of the digital intermediaries that have a dominant and decisive role in the way in which the information is accessed, consumed, prioritized, and remunerated (or not remunerated); 2) the order in which the criteria set in Article 22(2) should be considered, and their interplay; 3) the nature of the commitments to safeguard media pluralism and editorial independence, in case they are accepted as a condition to allow the media market concentration.

Moreover, we argued the rationale for a specific treatment of media mergers involving non-media actors and proposed to introduce guidelines that strongly disincentivize mergers giving control of the media to entities that have their prevalent business in other sectors, to strengthen the safeguards of editorial independence in times of media economic vulnerability. Finally, it is worth noting that the above-mentioned limits in the scope of Art. 22 could be addressed by the Member States in their national regulations. In fact, Art. 21 confirms the Member States powers and competences to take measures to safeguard media pluralism or editorial independence, so long as they are justified, respect proportionality principles, and are "reasoned, transparent, objective and non-discriminatory".

34. Baron 2025.

35. Baker 2007, p. 178.

References

S.P. Anderson, B. Julien (2015), *The Advertising-Financed Business Model in Two-Sided Media Markets*, Handbook of Media Economics, North Holland, vol. 1, 2015

C.E. Baker (2007), *Media concentration and democracy: why ownership matters*, Cambridge University Press, 2007

M. Baron (2025), *Where Jeff Bezos went wrong with The Washington Post*, in "The Atlantic", 3 March 2025

K. Bleyer-Simon, D. Da Costa Leite Borges, E. Brogi et al. (2024), *Monitoring media pluralism in the digital era : application of the media pluralism monitor in the European member states and in candidate countries in 2023*, EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), Country Reports, 2024

E. Brogi, D. Da Costa Leite Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Parliament, 2023

T. Burman (2025), *Donald Trump's Tech Bro Orbit—How Silicon Valley Merged With MAGA*, in "Newsweek", 13 January 2025

R. Carlini, P.L. Parcu (2024), *How article 22 aims to tackle market power in the platformed media environment. A critical test for European media*, Blogpost in EMFA Observatory, 18 December 2024

CMPF (2024), *Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023*, EUI, 2024

CMPF (2023), *Feedback on the proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU*, EUI, 2023

G. Doyle (2016), *Why ownership pluralism still matters in a multi-platform world*, in P. Valcke, M. Sükösd, R.G. Picard (eds.), "Media Pluralism and Diversity: Concepts, Risks and Global Trends", Palgrave Macmillan, 2016

European Commission - Directorate-General for Communications Networks, Content and Technology (2022), *Study on media plurality and diversity online – Final report*, Publications Office of the European Union, 2022

A. Fanta (2024), *25 years ago, Europe failed to curb the power of media moguls. It still haunts us today*, The EU files, Follow the Money, 13 January 2024

J. Furman, D. Coyle, A. Fletcher et al. (2019), *Unlocking Digital Competition. Report of the Digital Competition Expert Panel*, 2019

N. Just (2009), *Measuring media concentration and diversity: new approaches and instruments in Europe and the US*, in "Media, Culture & Society", vol. 31, 2009, n. 1

K. Karppinen (2013), *Rethinking media pluralism*, 1st ed., Fordham University Press, 2013

T. Kerševan (2024), *From rhetoric to regulation: EMFA and media concentration in the digital age*, in "Rivista italiana di informatica e diritto", 2024, n. 2

A. Manganelli, L. Mariniello (2024), *La valutazione delle concentrazioni per la tutela del pluralismo informative*, in "Rivista italiana di informatica e diritto", 2024, n. 2

Y. Montjoye, H. Schweitzer, J. Crémer (2019), *Competition policy for the digital era*, European Commission, Directorate-General for Competition, 2019

M. Moore, D. Tambini (eds.) (2018), *Digital dominance: the power of Google, Amazon, Facebook, and Apple*, Oxford University Press, 2018

C. Mymbs Nice (2025), *What Elon Musk is doing to the government*, in "The New Yorker", 26 February 2025

R.K. Nielsen, S.A. Ganter (2022), *The power of platforms: shaping media and society*, Oxford University Press, 2022

E.M. Noam (2016), *Who owns the world's media?: media concentration and ownership around the world*, Oxford University Press, 2016

Ofcom (2022), *Media plurality and online news. Discussion document*, 16 November 2022

Ofcom (2021), *Statement: the future of media plurality in the UK*, 17 November 2021

OECD (2021), *Competition issues concerning news media and digital platforms*, OECD Competition Committee Discussion Paper, 2021

P.L. Parcu (2019), *New digital threats to media pluralism in the information age*, EUI RSCAS, 2019/19

R.G. Picard, C. Dal Zotto (2016), *The dimension of ownership and control of media*, in P. Valcke, M. Sükösd, R.G. Picard (eds.), "Media pluralism and diversity: concepts, risks and global trends", Palgrave Macmillan, 2016

A. Prat (2020), *Measuring and Protecting Media Plurality in the Digital Age: A Political Economy Approach*, 10 August 2020

J. Schlosberg (2017), *Media ownership and agenda control: the hidden limits of the information age*, Routledge, 2017

T.J. Seipp, N. Helberger, C. de Vreese, J. Ausloos (2024), *Between the cracks: Blind spots in regulating media concentration and platform dependence in the EU*, in "Internet Policy Review", vol. 13, 2024, n. 4

M. Sznajder (2024), *Biting More Than It Can Chew. On the The EMFA's Media Pluralism Test*, Blogpost for Verfassungblog, 16 July 2024

Stigler Committee on Digital Platforms (2019), *Final Report*, The University of Chicago Booth School of Business, 20 January, 2025

Stigler Media Subcommittee (2019), *Protecting journalism in the age of digital platforms*, 16 September 2019

P. Valcke, M. Sükösd, R.G. Picard (eds.) (2016), *Media pluralism and diversity: concepts, risks and global trends*, Palgrave Macmillan, 2016

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0232 • articolo sottoposto a peer review • pubblicato in anteprima il 11 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Simone Calzolaio

Il principio del pluralismo rovesciato. Alla riscoperta dell'ordinamento costituzionale della politicità

Obiettivo del contributo è descrivere alcuni significativi mutamenti che connotano il principio costituzionale italiano ed europeo del pluralismo informativo e offrire elementi di carattere giuridico e costituzionale per inquadrare quanto sta avvenendo e per rilevare le difficoltà che l'ordinamento liberaldemocratico incontra nel costruire nuovi istituti, e/o anticorpi, per proteggersi dalla forma assunta dal virus della carenza di informazione, della difficoltà di approfondimento affidabile del contesto informativo e della difficoltà di promuovere e mantenere rapporti sociali vivaci e significativi – cioè un contesto verace della politicità – in assenza dei quali la stessa democrazia costituzionale diventa un simulacro di se stessa, artificiale, artificiosa, artefatta: un deep fake del pluralismo appunto.

Pluralismo informativo – Ordinamento costituzionale – Politicità – Libertà di pensiero

Diversity Reversed: Rediscovering the Constitutional Order of Politics

The aim of this contribution is to describe some significant changes that characterize the Italian and European constitutional principle of information diversity and to offer elements of a legal and constitutional nature to highlight the difficulties that the liberal democratic system encounters in building new institutions, and/or antibodies, to protect itself from the form assumed by the virus of the lack of information, the difficulty of reliably in-depth analysis of the information context and the difficulty of promoting and maintaining lively and significant social relationships – that is, a true context of politics – in the absence of which constitutional democracy itself becomes a simulacrum of itself, artificial, contrived: a deep fake of diversity precisely.

Information diversity – Constitutional rule of law – Politics – Freedom of thought

L'Autore è professore associato di Diritto costituzionale presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* a cura di Elda Brogi

Sommario: 1. Origine, oggetto, limiti del contributo. – 2. Il pluralismo informativo fra ordinamento italiano ed europeo: cosa ne sappiamo. – 3. Segue: dall'interconnessione alla iperconnessione. – 4. Segue: i caratteri giuridici del pluralismo dell'iperconnessione. – 5. In particolare: la sfera politica ed elettorale. – 6. Il pluralismo rovesciato: infosfera, *information overload* e libertà cognitiva. – 7. Il pluralismo di fronte ai rischi sistemici. Sicurezza cibernetica e IA generativa. Guerra e realtà ibrida. – 8. *Overload* normativo e *overload* istituzionale. Elogio del costituzionalismo e contro la burocrazia dell'informazione. – 9. Vulnerabilità e vivacità dell'ordinamento costituzionale della politicità e dell'informazione (Corte cost. sent. n. 44/2025).

1. Origine, oggetto, limiti del contributo

Il presente contributo rappresenta una evoluzione dell'articolo pubblicato all'esito del Convegno organizzato dal Co.re.com. Umbria e dal prof. Calvieri dell'Università di Perugia, avente ad oggetto il principio del pluralismo e la sua evoluzione, in particolare sotto il profilo del pluralismo informativo applicato alle competizioni elettorali e, più in generale, alla formazione dell'opinione politica delle persone e dei cittadini[1].

Tutti i punti che si intendono sviluppare sono affrontati in modo necessariamente sintetico, e quindi potenzialmente incompleto o parziale, poiché l'alternativa sarebbe un inevitabile approccio monografico, impraticabile in questa sede. Si tratta infatti di una introduzione al tema del principio del pluralismo informativo[2] nel contesto socio-tecnologico contemporaneo.

L'occasione del Convegno citato è stata propizia per sviluppare e inquadrare alcune considerazioni sul tema.

Obiettivo del contributo pertanto è descrivere alcuni mutamenti che connotano il principio costituzionale italiano ed europeo del pluralismo informativo, di offrire elementi di carattere giuridico e costituzionale per inquadrare quanto sta avvenendo e per rilevare le difficoltà che l'ordinamento liberaldemocratico incontra nel costruire nuovi istituti, e/o anticorpi, per proteggersi dalla forma assunta dal virus della carenza di informazione, della difficoltà di approfondimento affidabile del contesto informativo e della difficoltà di promuovere e mantenere rapporti sociali vivaci e significativi – cioè un contesto verace della politicità – in assenza dei quali la stessa democrazia costituzionale diventa un simulacro di se stessa, artificiale, artificiosa, artefatta: un *deep fake* del pluralismo appunto – e ci si scusa per il termine.

Da quanto precede sono chiari anche i limiti del contributo. Ci si confronta con le caratteristiche e le conseguenze giuridiche di un tema enorme e sfuggente. L'obiettivo pertanto è contribuire sommessamente a introdurre alle tematiche trattate, consapevolmente sapendo di non poter ripercorrere adeguatamente il principio del pluralismo informativo[3].

1. Si veda Calvieri 2025; Calzolaio 2025-a.
2. Il "pluralismo informativo" è una declinazione del più generale concetto di "pluralismo" (su cui v. Bobbio 2004, pp. 700-705) che si può intendere in senso politico, cfr. Matteucci 2001, p. 435 ss., non meno che in senso giuridico, cfr. ora Luciani 2023.
3. … ma fortunatamente è possibile rinviare alla partizione temporale elaborata da accorta dottrina, cfr. Donati 2018, parr. da 2 a 5.

2. Il pluralismo informativo fra ordinamento italiano ed europeo: cosa ne sappiamo

Il principio del pluralismo informativo affonda le sue radici nelle stesse basi filosofiche giusnaturaliste che giustificarono sin dall'inizio l'esigenza di superare il sistematico controllo di censura degli stampati[4] da parte delle autorità costituite, civili e religiose, e di riconoscere che la ricerca della verità – questa strana cosa che questi intellettuali della fine del '600 e del '700 ancora credevano essere l'esigenza vitale di ciascun essere umano – necessita del confronto, del dialogo, o come amavano dire allora della tolleranza[5] delle opinioni e delle manifestazioni altrui. L'argomento secondo la verità e, successivamente, l'argomento per la democrazia rappresentano basi filosofiche semplici e solide per fondare, insieme alla tutela della libertà individuale di espressione, anche la prospettiva, a tratti dialettica, del principio del pluralismo come valore costituzionale[6].

I principi – categoria cui bisogna sempre ricorrere con cautela[7] – si inverano quando sono messi alla prova, o sotto pressione, dall'esigenza di affrontare problemi nuovi ed evoluzioni impreviste.

Nella esperienza costituzionale italiana il principio del pluralismo informativo ha trovato la sua dimensione ed è stato protagonista di una intera stagione[8] in occasione del superamento del monopolio televisivo pubblico, a partire dalla metà degli anni settanta del secolo scorso.

È opportuno ricordare che fino a quel momento il principio del pluralismo informativo conviveva serenamente in un contesto di consolidato e costituzionalmente giustificato[9] monopolio pubblico del sistema radiotelevisivo – si opinava proprio

4. Si veda l'intero par. 2.1 del davvero essenziale contributo di Vigevani 2025, pp. 236 ss., spec. pp. 242-245, in cui si osserva: "nel Cinquecento che i poteri pubblici istituiscono e consolidano sistemi di controllo preventivo delle pubblicazioni. (…) L'invenzione della stampa (…) fu una rivoluzione anche dal punto di vista della risposta dei poteri pubblici, che per la prima volta sentirono l'esigenza di istituire apparati di intervento preventivo, per governare e indirizzare i flussi informativi che lo sviluppo tecnologico aveva così tanto esteso. In realtà, questa risposta non fu immediata, ma fu innestata dalla rottura dell'unità religiosa europea: come noto, è proprio con la controriforma che la Chiesa cattolica si dota di un capillare e complesso sistema censorio, a cui erano speculari, anche se meno efficaci e più frammentati, i sistemi adottati nelle realtà in cui si era diffusa la riforma. Di qui una lunga storia di tentativi dei poteri pubblici, civili e religiosi, di governare la circolazione del sapere critico. E infatti la libertà di pensiero nasce e si consolida, non a caso, proprio come libertà fondamentale del singolo "contro" il potere pubblico; e questa impostazione, che circonda di cautele l'intervento pubblico nel mercato dell'informazione ed è ostile a ogni forma di controllo pubblico sulla qualità e la direzione dei flussi informativi, è quella ancora oggi scolpita nelle costituzioni delle democrazie liberali".
5. Si veda a questo riguardo il pensiero di J. Locke, come recentemente ripubblicato in forma gratuita e accessibile dall'editore il Mulino, Battaglia 1962: "non è la diversità di opinioni (che è impossibile evitare), ma la mancata tolleranza verso coloro che sono di opinioni diverse (che si potrebbe, invece, concedere), a produrre tutte le agitazioni e le guerre avvenute nel mondo cristiano per motivi religiosi".
6. Cfr. Gardini 2021, p. 16, ove l'Autore giustamente ricorda il pensiero di Milton, Locke e Mill. Per una lettura arguta e radicale, ma poco nota, in tema di giustificazione del libero pensiero e della libertà di espressione, v. Collins 1713/2019.
7. … "non bisogna appoggiarsi troppo ai principi, perché poi si piegano", è un aforisma attribuito all'arguto Leo Longanesi, di cui appare sempre opportuno fare tesoro, specialmente in questo momento storico e nel confronto con le tecnologie digitali. È anche un aforisma che ben si attaglia alla evoluzione giurisprudenziale del giudice costituzionale in materia di soglie antitrust nel settore radiotelevisivo, a cavallo fra gli anni Ottanta e i primi anni del 2000 (cfr. sentt. 826/1988, 420/1994, 466/2002 su tutte): sia consentito rinviare per la descrizione di tale evoluzione normativa e giurisprudenziale a Calzolaio 2008.
8. Su cui si rinvia senz'altro ancora a Salvatore 1993.
9. Corte Cost., sent. n. 59 del 1960; cfr. Caretti–Cardone 2024, p. 120-124.

che il monopolio pubblico garantisse un maggior pluralismo dell'altrimenti inevitabile oligopolio[10].

3. Segue: dall'interconnessione alla iperconnessione

Fu l'interconnessione funzionale[11] a provocarne il brusco risveglio: procacciandosi le frequenze di tante emittenti locali si riusciva a trasmettere simultaneamente la stessa programmazione televisiva e la stessa pubblicità commerciale a livello nazionale: qualcuno aveva avuto l'intuizione fenomenale di riuscire a superare – all'italiana, si direbbe – l'incapacità dell'amministrazione e della politica nazionale di governare il superamento del monopolio statale e l'avvento di un sistema dell'informazione di dimensione nazionale plurale ma non automaticamente pluralista.

Allora arrivò il momento del grande sviluppo, giurisprudenziale, normativo e dottrinale del principio del pluralismo informativo[12].

La Corte costituzionale si è da quel momento esercitata molto sul principio del pluralismo e si potrebbero citare una folta serie di sentenze[13] del giudice delle leggi sul tema.

Forse è nella sentenza n. 826 del 1988 che si rinviene una trattazione analitica e una sorta di statuto del principio del pluralismo informativo (esterno ed interno) applicato al sistema radiotelevisivo ed alle sue esigenze regolatorie secondo Costituzione. In questa decisione si chiarisce che "il pluralismo dell'informazione radiotelevisiva significa, *innanzitutto*, possibilità di ingresso, nell'ambito dell'emittenza pubblica e di quella privata, di quante più voci consentano i mezzi tecnici, con la concreta possibilità nell'emittenza privata – perché il *pluralismo esterno* sia effettivo e non meramente fittizio – che i soggetti portatori di opinioni diverse possano esprimersi senza il pericolo di essere emarginati a causa dei processi di concentrazione delle risorse tecniche ed economiche nelle mani di uno o di pochi e senza essere menomati nella loro autonomia. *Sotto altro profilo*, il pluralismo si manifesta nella *concreta possibilità di scelta*, per tutti i cittadini, tra una molteplicità di fonti informative, scelta che non sarebbe effettiva se il pubblico al quale si rivolgono i mezzi di comunicazione audiovisiva non fosse in condizione di disporre, tanto nel quadro del settore pubblico che in quello privato, di programmi che garantiscono l'espressione di tendenze aventi caratteri eterogenei" (nostro il corsivo).

Aggiunge la Corte, a corollario di quanto sin qui affermato, che "l'efficacia di una simile disciplina ai fini indicati presuppone l'introduzione di un alto grado di *trasparenza degli assetti proprietari e dei bilanci dell'impresa di informazione e di quelle collegate*, trasparenza che incide pur sempre sul valore del pluralismo ed ha quindi rilievo costituzionale" (nostro il corsivo).

Si tratta qui del cd. pluralismo esterno che – come si può osservare – è composto di tre elementi che spetta alla Repubblica perseguire: apertura al massimo numero assentibile di emittenti sulla base delle possibilità tecniche (i.e.: garanzia della pluralità delle emittenti, in un contesto di garanzia delle differenti libertà editoriali) e, contemporaneamente, libertà di scelta dei cittadini/utenti fra questa necessaria molteplicità di fonti informative (libertà di informarsi, interesse ad essere informati in un sistema dell'informazione libero e plurale). Si tratta di profili che ben possono essere fra loro confliggenti in concreto: pluralità delle emittenti, libertà di espressione degli editori, libertà di informarsi e interesse ad essere informati dei cittadini[14].

10. L'indagine va allargata e approfondita, cfr. Gardini 2015, pp. 185-235, il quale osserva opportunamente, da un lato, che esiste un punto di vista europeo, ben distinto da quello statunitense, sull'intervento pubblico diretto e regolatorio nel sistema dell'informazione radiotelevisiva e, dall'altro, che "nelle democrazie dell'Europa occidentale, il monopolio pubblico viene concepito come mezzo per garantire il pluralismo delle idee e delle opinioni politiche". Sul tema v. anche Pavani 2012, e Pavani 2016, pp. 1-33.
11. Cfr. Calzolaio 2008 e dottrina ivi citata.
12. V. per tutti la grande opera di Pace–Manetti 2006, spec. p. 345 ss., p. 532 ss., p. 614.
13. Cfr. la evoluzione giurisprudenziale citata in Calzolaio 2008, e poi Corte cost., sent. 155/2002 su cui Grandinetti 2002, pp. 1315 ss., e più di recente Corte cost., sent. 206/2019 su cui Napolitano 2020, p. 141 ss.
14. La medesima Corte costituzionale, sent. 826/1988: "Per quanto riguarda l'emittenza radiotelevisiva privata si tratta di comporre il diritto all'informazione dei cittadini e le altre esigenze di rilievo costituzionale in materia

E per questo assume specifico rilievo il terzo elemento della trasparenza degli assetti proprietari (art. 21, c. 5, Cost., in riferimento alla stampa periodica), e cioè della conoscenza/conoscibilità da parte della collettività degli interessi concreti alla base degli indirizzi editoriali perseguiti da ciascun editore.

Il principio del pluralismo informativo esterno – come principio appunto – rappresenta lo strumento per tenere in equilibrio tutti questi aspetti potenzialmente confliggenti. Spetta al legislatore perseguire questo punto di equilibrio, peraltro mutevole nel tempo a seconda delle condizioni e della evoluzione del sistema dell'informazione: se il legislatore vi riesce, il principio è "effettivo", e il sistema dell'informazione tende al pluralismo, altrimenti è "fittizio", e il sistema dell'informazione può anche essere plurale, ma non per questo è pluralista.

Accanto al profilo esterno si colloca quello interno del pluralismo informativo: "compito specifico del servizio pubblico radiotelevisivo è di dar voce – attraverso un'informazione completa, obiettiva, imparziale ed equilibrata nelle sue diverse forme di espressione – a tutte, o al maggior numero possibile di opinioni, tendenze, correnti di pensiero politiche, sociali e culturali presenti nella società, onde agevolare la partecipazione dei cittadini allo sviluppo sociale e culturale del Paese, secondo i canoni di *pluralismo interno*. Ed ovviamente spetta al legislatore di provvedere a che il servizio pubblico disponga delle frequenze e delle fonti di finanziamento atte a consentirgli di assolvere i propri compiti".

La Corte precisa conclusivamente che "il pluralismo *in sede nazionale* non potrebbe in ogni caso considerarsi realizzato dal concorso tra un polo pubblico e un polo privato che sia rappresentato da un soggetto unico o che comunque detenga una posizione dominante nel settore privato": esattamente quanto si è verificato nei successivi 25 anni.

Queste sintetiche – ma dense! – indicazioni giurisprudenziali ci consentono di qualificare i caratteri del pluralismo informativo (PPI) così come lo conosciamo:

1) il PPI nasce per garantire che, alla massima espansione dell'esercizio della libertà di manifestazione del pensiero in un ordinamento democratico, da parte di tutte le individualità che ne sono titolari (persone, giornalisti, editori, imprese culturali, ecc.), corrisponda un sistema dell'informazione libero e plurale, che a sua volta è condizione del permanere della possibilità di libera formazione del pensiero, della libertà di pensiero e, infine, di manifestazione del pensiero;
2) il PPI si sviluppa in un contesto tecnologico in cui vi è scarsità di frequenze radiotelevisive o di canali informativi e solo un numero ristretto di operatori può ambire a occupare frequenze e a trasmettere in chiaro sull'intero territorio nazionale;
3) il PPI necessita dell'intermediazione del legislatore e della gestione amministrativa della attribuzione delle frequenze (cioè della burocrazia) per essere attuato, poiché di norma non si realizza *spontaneamente* nell'ordinamento costituzionale;
4) il PPI esterno ha come obiettivo garantire un sistema dell'informazione plurale nella sostanza editoriale, culturale e ideale, non solo nel numero degli operatori in concorrenza economica fra loro[15] e quindi si avvale della, ma non si riduce alla messa in concorrenza degli attori del sistema dell'informazione (condizione necessaria, ma non sufficiente sul piano del pluralismo)[16];
5) il PPI ha anche una dimensione interna, che vale per tutti gli attori del sistema dell'informazione, ma segnatamente per quelli che sono finanziati o sono sotto il controllo pubblico[17]

con le libertà assicurate alle imprese principalmente dall'art. 21, oltre che dall'art. 41 Cost., in ragione delle quali il pluralismo interno e l'apertura alle varie voci presenti nella società incontra sicuramente dei limiti. Di qui la necessità di garantire, per l'emittenza privata, il massimo di pluralismo esterno, onde soddisfare, attraverso una pluralità di voci concorrenti, il diritto del cittadino all'informazione".

15. È la distinzione fra *diversity* (pluralismo, appunto) e *plurality* (concorrenza) ben delineata in dottrina da Pampanin 2019, p. 381 ss.
16. Cfr., con chiarezza, Gardini 2021, p. 19 ss.
17. Utilissimo e chiarissimo in questo senso il contenuto del par. 6.4 (le situazioni sintomatiche verso lo Stato e verso gli organi di comunicazione e d'informazione) del manuale di Zaccaria–Valastro–Albanesi 2023, che

e devono garantire una effettiva dimensione pluralista della informazione del servizio pubblico.

Vi è un ultimo aspetto che l'esperienza italiana del PPI nel settore radiotelevisivo ci consegna, e ci insegna: in modo discontinuo, imperfetto e non sempre sufficientemente incisivo, il legislatore, il giudice costituzionale, la magistratura ordinaria e amministrativa, l'Autorità di settore – e perfino il popolo attraverso l'utilizzo dell'istituto referendario – hanno perseguito una applicazione significativa del PPI[18]. Tuttavia, non sono mai riusciti o, forse meglio, non hanno mai inteso conseguire in modo dirigistico e unilaterale l'applicazione del PPI, superando il duopolio televisivo con modalità che non corrispondessero ad una effettiva evoluzione del sistema radiotelevisivo e del sistema dell'informazione nel suo complesso[19].

Ciò in quanto l'intervento normativo e burocratico dello Stato nel settore della libertà di espressione e del sistema dell'informazione è un intervento rischioso per sua stessa natura, ove proprio l'obiettivo della correzione di storture all'applicazione del PPI può facilmente divenire una stortura esso stesso e pertanto deve mantenersi prudentemente coerente con l'impostazione dell'art. 21 Cost. "che attribuisce alla Repubblica il compito di garantire la pluralità dei mezzi di comunicazione e la trasparenza della proprietà dei medesimi, al fine di limitare i poteri privati e assicurare la concreta possibilità delle diverse idee di esprimersi e circolare, ma che individua, comunque, nello Stato il pericolo maggiore per il dispiegarsi di un libero confronto che conduca, secondo la lezione di grandi pensatori moderni, a una verità necessariamente relativa, parziale, incerta, effimera, convenzionale, che deve nascere da circuiti diversi da quello politico"[20].

4. Segue: i caratteri giuridici del pluralismo dell'iperconnessione

È abbastanza evidente che alcuni dei caratteri di fondo del principio del pluralismo informativo mutano con l'avvento della banda larga e ultralarga (più ancora che della rete Internet in sé considerata), che ha consentito lo sviluppo dell'Internet c.d. 2.0 e oltre[21].

Il problema della limitatezza dei canali informativi è oggi un ricordo del passato, così come il problema dell'oligopolio informativo (inteso nel senso in cui se ne discuteva, *in sede nazionale*, fra gli anni Ottanta e gli anni Duemila), così come il problema della garanzia di esercizio individuale della libertà di manifestazione del pensiero della persona. Ciò non significa che il PPI sia stato conseguito – e per inciso si ritiene che il PPI non si possa neanche conseguire, in termini ideali, trattandosi di un punto di equilibrio e non di un assoluto.

Con ciò si vuole solo osservare – descrittivamente – che il PPI non si confronta più con i caratteri del sistema dell'informazione che erano noti, studiati, regolati e dibattuti vivacemente in ogni sede fino a circa dieci anni fa.

Si tornerà ovviamente sul punto, ma la prima acquisizione raggiunta è a mio avviso la seguente: il PPI è stato affinato ed ha informato di sé l'ordinamento costituzionale nell'affrontare il problema dell'interconnessione funzionale, cioè di un sistema dell'informazione radiotelevisiva nato da un *escamotage*, che aveva convogliato, moltiplicato e prosciugato le risorse pubblicitarie del sistema dell'informazione ed era cresciuto come un fungo sotto l'albero del monopolio radiotelevisivo pubblico, mettendo a rischio – ma mai sopprimendo – la libertà di e dell'informazione in Italia in quei decenni.

Quel problema del sistema radiotelevisivo italiano, così come lo si conosceva ed era affrontato

delineano proprio le fattispecie in cui si concretizza quello che gli AA. qualificano come diritto sociale all'informazione (par. 6.3).

18. Cfr., *ex multis*, Calzolaio 2008.

19. Ricorda opportunamente che il PPI non si è realizzato neanche dopo l'avvento del digitale terrestre Manetti 2012, come recentemente ricordato da Borrello 2019, p. 237.

20. Vigevani 2025, pp. 236 ss., spec. pp. 241.

21. Cfr. Caravita di Toritto 2023, p. 27 ss.

e viene tutt'ora regolato, non è più attuale ed è al massimo residuale[22].

Sul piano quantitativo e qualitativo il PPI si confronta oggi con un tema diverso, che ancora una volta si identificherà con termine volutamente sintetico: l'iperconnessione.

Dall'interconnessione all'iperconnessione è un'immagine che vuole significare che la caratteristica attuale del sistema dell'informazione risiede nella pervasività, immersività, ambiguità (comunicazione o informazione?), individualità (*on demand*!), velocità del modello della comunicazione digitale che coinvolge l'intera collettività, con i minori in primissima linea[23].

Se il contesto in cui il PPI è stato messo alla prova era caratterizzato dalla scarsità di canali informativi, dalla concentrazione di potere informativo e dalla conseguente potenziale difficoltà a reperire fonti di informazione da parte dell'individuo, oggi il problema con cui si confronta il PPI è la difficoltà individuale e collettiva a reggere l'urto emotivo e cognitivo della quantità delle informazioni che ci raggiungono, di capirne l'affidabilità e l'origine (umana o sintetica), di liberarsi dalla calamita (e dalla calamità) delle informazioni suggerite (sistemi di raccomandazione) basate sulle "nostre" preferenze (così come classificate da algoritmi e cluster in cui siamo profilati), mantenendo spazi di effettiva autonomia cognitiva, di riflessione personale e di genuina partecipazione sociale.

L'iperconnessione, infatti, genera solitudine e isolamento[24], e poi smarrimento e polarizzazione, infine menzogna e violenza.

Il pluralismo informativo è chiamato ad affrontare questa condizione attuale e quindi a rivedere i propri strumenti: dalla lotta alla scarsità al contrasto all'eccesso, dalla protezione *del* sistema dell'informazione alla tutela *dal* sistema dell'informazione[25], dalla protezione della libertà di manifestazione del pensiero alla tutela della libera formazione del pensiero[26], e così via descrivendo.

Va sottolineato che il patrimonio di istituti di cui si compone il PPI è stato formato, nei secoli, per affrontare i vecchi problemi di censura (pubblica), e poi scarsità e limitatezza di canali trasmissivi e informativi. Molti di questi istituti – si pensi al tema della trasparenza negli assetti proprietari – si rivelano tutt'altro che superati. Ma solo ora ci si avvia ad un percorso di verifica e aggiornamento degli istituti neceessari ad inverare il vecchio PPI nel nuovo contesto della società digitale.

Non è un caso che gli osservatori più acuti si domandano se sono ancora attuali le nostre categorie concettuali[27], osservano che la tutela del pluralismo è alla ricerca di una propria identità[28] e concludono affermando la "necessità di ripensare il concetto di pluralismo"[29] (e con esso di *discorso pubblico*[30]).

È proprio così. In questo momento il principio del pluralismo informativo somiglia – lo si dice rispettosamente – al dio ignoto che San Paolo annuncia nell'Aeròpago agli ateniesi, che lo adorano senza conoscerlo, che si cerca se mai si arrivi a trovarlo come a tentoni, benché non sia lontano da ciascuno di noi[31]. È qualcosa che conosciamo, ma a cui ancora non riusciamo a dare forma (attuale) e (nuova) sostanza.

22. … autorevole dottrina è di opinione diversa: cfr., *ex multis*, Vigevani–Cazzaniga 2024, pp. 28-29.
23. Cfr. Calzolaio 2023-a, p. 291 ss.
24. Si veda, Calzolaio 2023.
25. Cfr. Sunstein 2021, il quale ricorda l'opinione espressa dal giudice della Corte Suprema statunitense Robert Jackson e ci avverte che "Those who begin coercive elimination of dissent soon find themselves exterminating dissenters. Compulsory unification of opinion achieves only the unanimity of the graveyard." (causa *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 641 (1943)).
26. Più acutamente e prima di molti altri: Richards 2015.
27. Pitruzzella 2017, pp. 46-47.
28. Apa 2021, p. 251.
29. Cuniberti 2017, p. 26 ss., intitola così il par. 3.4, conclusivo del suo saggio.
30. Cfr. Caruso 2013, pp. 81 ss. e 145 ss.
31. Cfr. Atti degli Apostoli, 17,22-28, anche in *https://www.bibbiaedu.it/CEI2008/nt/At/17/*.

E così – vedremo – si spiega buona parte dell'*e-scalation* normativa europea, che coinvolge anche il ruolo dell'AGCOM[32].

5. In particolare: la sfera politica ed elettorale[33]

Non vi è un esempio più maturo della concezione tradizionale del pluralismo informativo applicato alla sfera politico-elettorale[34] della l. 22 febbraio 2000, n. 28[35].

In questa sede non è sensato ripercorrere la disciplina della legge citata, ma quel che interessa osservare – in scia con la dottrina che lucidamente ha approfondito questo aspetto[36] – è l'impostazione strutturale della disciplina legislativa: essa è volta a regolamentare l'accesso ai canali di informazione radiotelevisiva in un'ottica paritaria e per questo disciplina il tema dell'equità di accesso delle forze politiche ai mezzi radiotelevisivi nazionali e locali intendendoli come una risorsa scarsa, che spetta al legislatore aprire in modo equo e gratuito alle forze politiche, col concorso delle Autorità di settore (AGCOM e Commissione parlamentare di vigilanza).

L'articolata (e occhiuta) disciplina della comunicazione politica (artt. 2, 3 e 4) e poi della informazione di rilievo politico (artt. da 5 a 9), si giustifica proprio come applicazione del modello del pluralismo informativo, esterno e interno, dell'epoca dell'interconnessione e della scarsità di frequenze, con poche e ben canalizzate informazioni disponibili: il problema del pluralismo informativo è quindi un problema di libertà del sistema dell'informazione, inteso quest'ultimo come "infrastruttura" pubblica e privata, nazionale e locale, una *turris eburnea* titolare dei canali informativi di massa che irradia la società e di cui quindi deve essere garantita dal legislatore l'apertura alle forze politiche in condizioni di parità fra loro.

Ecco, quindi, che il "pluralismo" si garantisce "attraverso la parità di trattamento, l'obiettività, l'imparzialità e l'equità nella trasmissione sia di programmi di informazione, nel rispetto della libertà di informazione, sia di programmi di comunicazione politica" (così, in riferimento all'emittenza locale, l'art. 11-*quater*, l. n. 28/2000).

Questa è appunto la formulazione normativa del PPI tradizionale, che si basa sulla pretesa legislativa di regolare e controllare forma e contenuto del fenomeno comunicativo a ridosso delle consultazioni politiche (di cui all'art. 1, c. 2), pretesa fondata a sua volta sulla natura pubblica di un pezzo del sistema dell'informazione e sul sistema concessorio della attribuzione delle frequenze per la parte privata, nazionale e locale, cui quindi possono essere imposti obblighi e oneri[37].

L'avvento della banda larga e, con essa, della larga e progressiva diffusione dei social media, ha condotto al fenomeno dell'iperconnessione e ad un nuovo modello di sistema dell'informazione (e d'informazione politica). È all'interno di questo nuovo ecosistema che si fonda, consolida e indirizza la visione politica e la persuasione al voto. Questo modello ha superato lo schema normativo della l. 28/2000, che attualmente è – almeno – incompleto, ma più realisticamente va radicalmente ripensato, facendo lo sforzo non di trovare principi nuovi, ma di attualizzare i vecchi principi del pluralismo informativo.

32. Cfr. Orofino 2024, spec. p. 164 ss.
33. Sul tema si rinvia agli approfonditi e competenti contributi di O. Grandinetti, fra i quali più di recente, e con taglio ricostruttivo, Grandinetti 2019, p. 201 ss.
34. Per l'inquadramento costituzionale del diritto di voto, sempre utile Rubechi 2016.
35. Per l'inquadramento e i precedenti normativi v. per tutti Gardini 2021, p. 80 ss.
36. *Ibidem*.
37. Ciò comporta – segnala l'AGCOM – che non rientrano nell'ambito di applicazione della l. n. 28/00 soggetti che trasmettono in chiaro ma che non erano, al tempo dell'entrata in vigore (non della promulgazione, come osserva invece il doc. AGCOM) della legge 28/00, "concessionarie analogiche", cfr. AGCOM 2023, pp. 19-21.

Di ciò si è evidentemente avveduta accorta dottrina[38], oltre che l'AGCOM[39].

E quindi si comincia a profilare l'evoluzione del principio pluralista nell'epoca dell'iperconnessione[40].

Infatti – ferma, immobile la l. n. 28/00 – la del. AGCOM n. 90/24/CONS recante *Disposizioni di attuazione della disciplina in materia di comunicazione politica e di parità di accesso ai mezzi di informazione relative alla campagna per l'elezione dei membri del Parlamento europeo spettanti all'Italia fissata per i giorni 8 e 9 giugno 2024* contiene un Titolo VI (*Piattaforme per la condivisione di video e social network*) con un solo art. 30 (*Tutela del pluralismo sulle piattaforme online*), il quale richiama le piattaforme ad assicurare il rispetto del principio del pluralismo informativo e ad adottare misure di contrasto al fenomeno della disinformazione secondo gli orientamenti europei contenuti nel codice di condotta sulla disinformazione 2022 e soprattutto negli *Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del regolamento (UE) 2022/2065*.

Nel regolamento si estendono espressamente alle piattaforme online i vincoli concernenti il divieto di pubblicazione dei sondaggi politici ed elettorali ed il regime della comunicazione istituzionale di cui agli artt. 8 e 9 l. 28/00.

Ma soprattutto, leggendo l'art. 30, c. 2, si scorge – pur senza apposita e idonea base legislativa e nel quadro ormai vieppiù ristretto della l. n. 28/00 – la nuova dimensione del pluralismo informativo al tempo dell'iperconnessione, ove pertanto assume rilievo assicurare "la previsione di *attività di fact-checking* da parte di organizzazioni indipendenti, la *trasparenza* e la *riconoscibilità* dei profili o account social provenienti direttamente o indirettamente da Paesi Terzi, la *chiara identificazione* dei messaggi politici a pagamento, l'adozione di strumenti di *mitigazione* relativi ai contenuti disinformativi prodotti dall'intelligenza artificiale *generativa*" (nostro il corsivo).

Inoltre si richiede alle piattaforme di assicurare "l'accesso a informazioni ufficiali sul processo elettorale", di promuovere "iniziative di educazione ai media" e di garantire "la moderazione dei contenuti che minacciano l'integrità del processo elettorale".

Questi contenuti normativi non erano presenti nella precedente delibera AGOCM sulle elezioni politiche del 2022.

Ovviamente si tratta solo – sul piano della tenuta e della efficacia giuridica – dell'avvio di un percorso di attualizzazione del PPI. Ma era inevitabile, oltre che necessario, iniziare. Come si può osservare, *fact-checking*, trasparenza e riconoscibilità dei profili, chiara identificazione, mitigazione, sono tutti concetti evolutivi del vecchio modulo del pluralismo informativo e caratteristici del pluralismo informativo che deve proteggere la fase della formazione del pensiero dalla iperconnessione.

6. Il pluralismo rovesciato. Infosfera, *information overload*[41] e libertà cognitiva

Eccoci quindi giunti allo snodo del nostro discorso. Dopo la cd. quarta rivoluzione e con l'avvento dell'infosfera[42] – che qui volutamente si indicano come patrimonio concettuale comune – "il problema centrale del pluralismo, oggi, non è più tanto dare uno spazio a tutti (posto che lo spazio è quasi

38. Cfr. da ultimo Vigevani–Cazzaniga 2024, p. 14 ss.; v. in precedenza anche Donati 2019; Biondi Dal Monte 2018. Per la descrizione dei nuovi paradigmi della comunicazione politico-elettorale v. Allegri 2020, p. 19 ss., così come per l'analisi dell'aggiornamento delle discipline in materia da parte di altri paesi europei, p. 113 ss. Per la dimensione più generale e sistemica: Di Cosimo 2023.
39. Cfr. del. n. 423/17/CONS, recante Istituzione di un tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali, e la successiva pubblicazione in vista delle diverse consultazioni elettorali di doc. recanti gli "Impegni assunti dalla società esercenti le piattaforme on line per garantire la parità di accesso dei soggetti politici alle piattaforme digitali durante la campagna elettorale" a partire dal 2019.
40. Cfr. anche Martusciello 2019, p. 47 ss.
41. Bawden–Robinson 2020.
42. Floridi 2014.

illimitato), quanto fare in modo che ciascun soggetto venga concretamente a contatto con una pluralità di opinioni diverse"[43].

Bisogna soffermarsi su questa osservazione.

Abbiamo fatto sistematico riferimento, in estrema e brutale sintesi, alla cd. iperconnessione.

Possiamo ora specificare che nell'infosfera siamo immersi in una quantità spropositata di informazioni che ci colpiscono e ci avvolgono con ineluttabile continuità, in modo veloce, immediato (in senso etimologico: non mediato da nulla), che supera la nostra capacità di assimilazione e riflessione; per questo viene sollecitata la reattività e l'emotività, non il *discorso* pubblico – anche radicale, se si vuole – ma meditato.

Bisogna ora aggiungere alcuni ulteriori elementi fattuali:

- questa quantità immersiva di informazioni produce – in apparente paradosso – disinformazione nelle persone e nelle collettività, classificabile sotto diversi profili (disiniformazione, misinformazione, malinformazione)[44];
- in particolare, si parla al riguardo di *information overload*, nozione che si basa su un concetto di informazione/i diverso rispetto al classico significato di "informazione-notizia-cronaca" o "informazione-opinione-critica" che si utilizza nel tradizionale sistema dell'informazione analogica: "informazione" è anche quella apparente comunicazione individuale, magari impersonale, che arriva da chissà chi – torniamo a breve sul punto – attraverso i social media o via email o come notifica in quel preciso orario e con quel preciso contenuto, che tocca la nostra emotività (il nostro "stato d'animo") prima ancora che possa attivarsi una forma di riflessione cosciente; in questo ambito si discute proprio cosa debba intendersi per "informazione" nel caso di information overload: dati, documenti, contesti immersivi, idee, ideologie – e anche su questo si tornerà;
- molto interessante, ai nostri fini, l'esito di questo sovraccarico informativo, perché ci riporta al nostro tema: l'information overload conduce di norma all'impossibilità di assimilazione consapevole delle informazioni e quindi alla cd. "povertà informativa".

Osserviamo che il PPI nasce come rimedio alla scarsità di canali di informazioni ed al rischio di oligopoli informativi perché creano "povertà informativa" ed oggi rappresenta, invece, lo strumento per affrontare il problema della povertà informativa derivante dall'eccesso di esposizione alle informazioni[45].

È, appunto, il pluralismo rovesciato: afferma Harari che "in the past, censorship worked by blocking the flow of information. In the twenty-first century, censorship works by flooding people with irrelevant information. We just don't know what to pay attention to, and often spend our time investigating and debating side issues. In ancient times having power meant having access to data. Today having power means knowing what to ignore"[46].

Gli evidenti anacronismi della legge sulla *par condicio* ci dimostrano che pian piano veniamo comprendendo la natura dei problemi che abbiamo di fronte, ma con ogni evidenza non abbiamo ancora strumenti adeguati per affrontarli: non sappiamo esattamente quale livello politico e normativo dovrebbe disciplinare la materia; non sappiamo esattamente quale autorità è adeguata ad occuparsene ed in quale modo; non sappiano esattamente neanche quali dovrebbero essere contenuti e istituti del nuovo modello pluralista e quali ambiti dovrebbe toccare. Procediamo a tentoni, o per tentativi.

Osserviamo empiricamente però che il PPI – nonostante l'elevato numero di fonti dell'informazione e la quasi assoluta libertà di espressione individuale – è a forte rischio, specialmente per quanto attiene alla comunicazione politica, che implica anche il rischio di tenuta degli ordinamenti democratici[47].

43. Cuniberti 2017, p. 39.
44. Molto utile, per comprendere, il Rapporto del Consiglio d'Europa: cfr. Wardle–Derakhshan 2017; cfr. Wang–McKee–Torbica–Stuckler 2019.
45. Cfr. Montaldo 2020, p. 22
46. Così Harari 2016, p. 324.
47. Non si può qui approfondire il recente caso rumeno, su cui si rinvia a Rosa 2025, p. 53 ss.

Fra i molteplici aspetti, ve ne sono due che a mio avviso vanno evidenziati per contribuire alla costruzione del *principio del pluralismo rovesciato* e dei suoi istituti.

In primo luogo, se il pluralismo – come è evidente – è messo a rischio dal sovraccarico informativo, si può facilmente rilevare che l'eccesso di informazione si muove pressoché interamente attraverso il canale digitale: in altri termini, il sovraccarico di informazione è la proiezione del processo di datificazione[48] nel rapporto fra ecosistema digitale e persona/società civile. Ciò implica che vi sia uno stretto legame fra tutela del pluralismo nelle società contemporanee e "diritto dei dati": la protezione del pluralismo passa per un insieme di discipline giuridiche che, sotto profili e in ambiti diversi, regolamentano l'utilizzo dei dati e limitano il potere dei soggetti che, attraverso lo sfruttamento dei dati, esercitano una grande influenza sulle persone e sulla società.

Il primo e più evidente livello di questa influenza – come dimostrano gli psicogrammi di Cambridge Analytica[49] – è la vulnerabilità cognitiva[50], ovvero – in termini giuridici – la minaccia alla libertà di formazione del pensiero delle persone, segnatamente del pensiero politico *latu sensu*[51], che si sviluppa attraverso la profilazione e la manipolazione psicologica e subliminale, determinata non solo da modelli, soggetti o intenti malevoli, ma specificamente caratteristica della vita in ambiente digitale, che implica sempre una certa dose di tracciamento, di profilazione dei comportamenti, di osservazione delle ricerche, di analisi delle abitudini di lettura, di classificazione esterna delle comunicazioni personali.

Vi è un nesso, pertanto, fra tutela del pluralismo e *intellectual privacy*[52], cioè protezione della sfera intima della formazione del pensiero da intrusioni indesiderate (sul piano personale) e indesiderabili (sul piano sociale e costituzionale), svolte da chi ha il potere di profilarci e lo usa per manipolarci. Senza che ce ne accorgiamo. Questa dimensione ultima della cd. privacy – che dal diritto alla riservatezza, passando per l'*informational privacy* (diremmo noi, autodeterminazione informativa), arriva ora alla privacy dell'intelletto[53] – si collega immediatamente all'altra evoluzione qui sommessamente introdotta del pluralismo informativo rovesciato.

Il secondo aspetto che si ritiene ineludibile mettere in luce concerne il *continuum* che si realizza nell'odierno sistema dell'informazione fra social media e media tradizionali (e le sue più che vistose conseguenze sulla disciplina in materia di concentrazioni in ambito di media audiovisivi).

I rapporti Censis sulla comunicazione[54] documentano che vi è ormai una compenetrazione fra la vecchia, ma longeva e coriacea, TV e l'informazione digitale: "ad un ascolto lineare e famigliare di un palinsesto unico e uguale per tutti si è sostituito un ascolto più erratico e individualizzato, in cui ciascuno può trovare ovunque e in ogni momento della giornata i contenuti che lo interessano "estraendoli" dalle diverse piattaforme, in modalità lineare e online, in diretta e in differita, per intero o per pillole"[55]. In altri termini, la TV *nella* società

48. Su questo processo sia consentito rinviare a Calzolaio 2017, p. 597 ss.
49. Origgi 2018, p. 455: "La psicografia, la nuova tecnologia che ha rivoluzionato il marketing negli ultimi anni, è un po' come la demografia, ma aggiunge alle informazioni sullo stato civile di una persona (età, indirizzo, professione), che sono da sempre pubbliche, informazioni sulle sue abitudini: "si preoccupa del suo aspetto fisico", "ama la musica rap", "vuole uno stile di vita sano, ma non ha molto tempo per lo sport e le diete", etc. Questo "profilo psicografico" può essere inferito a partire dai dati di navigazione online di una persona, le tracce che lascia sulle reti sociali, gli acquisti online e i suoi movimenti se usa un telefono cellulare. Attraverso la classica tecnica statistica di analisi di regressione, si riescono a stimare le relazioni tra le differenti variabili, costruire un profilo psicografico e fare predizioni sui comportamenti futuri".
50. *Ivi*, p. 447.
51. Cfr. Meola 2020, p. 84 ss.
52. Cfr. per la teorizzazione giuridica del tema: Richards 2015, e volendo Calzolaio 2018.
53. … sia consentito rinviare a Calzolaio 2017, p. 610 ss.
54. Si veda Censis 2023.
55. Così Italia 2024, p. 20 ss.

connessa è la TV *della* società connessa[56], in cui per l'appunto la TV è un importante "continente" della società connessa, ma in un "mondo" dell'informazione ormai determinato dall'infrastruttura di Internet e dalla comunicazione in ambiente digitale.

Non ha molto senso continuare a intendere la TV come il principale veicolo dell'informazione, inteso in senso "isolato ed autonomo" dalla società connessa.

Di ciò si è avveduta, con una decisione in parte sottovalutata[57], la CGUE[58] che nel 2020 ha chiaramente statuito su due aspetti: il primo attiene al valore "costituzionale" europeo (*ex* art. 11, par. 2, Carta dei diritti fondamentali Ue) del principio del pluralismo, la tutela del quale è indubbiamente uno di quei motivi imperativi di interesse generale che consentono – in astratto – di limitare l'altrimenti intangibile e preminente libertà di stabilimento (cfr. pp. 54-57).

Il secondo profilo attiene alla congruità (e proporzionalità) del paniere contemplato dal Sistema integrato delle comunicazioni (SIC) a determinare le soglie di concentrazioni adeguate a poter ledere il principio del pluralismo informativo e, di conseguenza, a limitare legittimamente la libertà di stabilimento. A tal riguardo la CGUE statuisce che "limitando la definizione del settore delle comunicazioni elettroniche ai mercati suscettibili di regolamentazione *ex ante*, la disposizione di cui al procedimento principale, come interpretata dall'AGCOM, esclude dal settore delle comunicazioni elettroniche *mercati di importanza crescente per la trasmissione di informazioni*, vale a dire i servizi al dettaglio di telefonia mobile e altri servizi di comunicazione elettronica collegati ad Internet nonché i servizi di radiodiffusione satellitare. Ebbene, essi sono divenuti la "principale via di accesso ai media, cosicché non è giustificato escluderli da tale definizione"[59].

Al di là di considerazioni specifiche attinenti al caso di specie[60], appare chiara l'indicazione di merito al legislatore italiano (superare l'attuale obsoleto paniere del SIC) e altrettanto chiara appare l'indicazione più generale: il vecchio mercato radiotelevisivo è ormai economicamente residuale nel sistema dell'informazione "connesso", dominato da Internet e dai suoi servizi.

Ecco quindi che "le piattaforme online svolgono un ruolo sempre più importante non soltanto a livello economico, ma anche nel campo dell'informazione e della comunicazione"[61], ponendo uno specifico problema in termini di pluralismo delle fonti informative, che il legislatore europeo ha indubbiamente colto.

Non si possono qui passare in rassegna i contenuti delle disposizioni europee che sono state adottate nell'ultimo biennio: tuttavia si può facilmente osservare che di fronte all'overload informativo, l'Unione si è mossa con un overload normativo, anticipando di molto una effettiva e comprensiva

56. *Ivi*, p. 20.

57. Ma v. con puntualità e obiettivo anticipo, invece, Borrello 2017, p. 68 ss.

58. Cfr. CGUE, sez. V, sent. 3 settembre 2020, in c-719/18 (*Vivendi SA c. AGCOM e nei confronti di Mediaset SpA*), su cui Apa 2021; Orofino 2020, p. 201 ss.

59. Aggiunge la Corte subito dopo che: "per quanto riguarda, poi, la soglia del 10% dei ricavi complessivi del SIC, menzionata dalla disposizione di cui al procedimento principale, occorre osservare che il fatto di conseguire o meno ricavi equivalenti al 10% dei ricavi complessivi del SIC non è di per sé indicativo di un rischio di influenza sul pluralismo dei media. Infatti, dall'articolo 2, paragrafo 1, lettera s), del TUSMAR risulta che il SIC comprende mercati diversi e vari. Pertanto, se i ricavi complessivi realizzati da un'impresa nel SIC dovessero essere concentrati in uno solo dei mercati che compongono tale sistema in modo tale che la quota raggiunta in tale mercato sia nettamente superiore al 10% ma, qualora venga preso in considerazione l'insieme dei mercati che compongono il SIC, rimanga inferiore al 10%, il fatto che la soglia del 10% dei ricavi complessivi del SIC non venga raggiunta non potrebbe escludere qualsiasi rischio per il pluralismo dei media. Analogamente, nel caso in cui la soglia del 10% dei ricavi complessivi del SIC fosse sì raggiunta, ma tale 10% di ricavi si ripartisse tra ciascuno dei mercati che compongono il SIC, né il raggiungimento né lo sforamento di tale soglia del 10% costituirebbero necessariamente un pericolo per il pluralismo dei media".

60. Per il seguito anche normativo della vicenda, v. Grandinetti 2022, che introduce al nuovo art. 51, TUSMA.

61. Così Donati 2024, p. 235.

definizione e comprensione delle strade da intraprendere per la tutela del pluralismo informativo rovesciato.

Il *Digital Markets Act*[62] vuole proteggere la contendibilità e l'equità dei mercati in cui sono presenti i gatekeeper[63] della rete Internet "a vantaggio degli utenti commerciali e degli utenti finali" (art. 1, par. 1); anche se il pluralismo informativo rimane estraneo agli obiettivi perseguiti[64], il DMA, in qualche modo, vuol rappresentare un cordone sanitario nei confronti di oligopoli che possono limitare il mercato digitale, e vorrebbe prestarsi ad avere effetti indirettamente positivi proprio sul pluralismo.

Il *Digital Services Act*[65] pone invece norme per regolare i servizi digitali nel mercato unico, e si occupa abbastanza specificamente di pluralismo informativo, sotto diversi profili, primo fra tutti sotto la specie di obblighi per le piattaforme online e di motori di ricerca di dimensioni molto grandi[66], anche sotto il profilo della lotta alla disinformazione. Particolare importanza assume la relazione fra l'attività delle grandi piattaforme e i cd. "rischi sistemici", delineata nei cons. da 79[67] a 88. I rischi sistemici sono suddivisi in 4 categorie, e la tutela del pluralismo rientra espressamente nella seconda di esse (cons. 81). Va sottolineato – ai fini dell'impostazione del nostro discorso – che i "rischi sistemici" sono ampiamenti richiamati e utilizzati per determinare obblighi e adempimenti in capo alle grandi piattaforme[68], ma curiosamente non rientrano nel novero delle definizioni offerte dal DSA all'art. 2, pur essendo in qualche modo classificati nell'art. 34.

62. Reg. (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).
63. Tutta la disciplina del DMA è fondata sulla qualificazione e classificazione dei Gatekeeper: cfr. Capo II, artt. 3 ss., e poi Capo III, artt. 5 e ss.
64. Cfr. Donati 2024, p. 241.
65. Reg. (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).
66. Cfr. il Capo III (Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro), Sez. 5 ("Obblighi supplementari a carico dei fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici").
67. … a mente del quale "Le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi possono essere utilizzati in un modo che influenza fortemente la sicurezza online, la definizione del dibattito e dell'opinione pubblica nonché il commercio online. La modalità di progettazione dei loro servizi è generalmente ottimizzata a vantaggio dei loro modelli di business spesso basati sulla pubblicità e può destare preoccupazioni per la società. Sono necessarie una regolamentazione e un'esecuzione efficaci al fine di individuare e attenuare adeguatamente i rischi e i danni sociali ed economici che possono verificarsi. Ai sensi del presente regolamento i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi dovrebbero pertanto valutare i rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'uso dei loro servizi, nonché dai potenziali abusi da parte dei destinatari dei servizi, e dovrebbero adottare opportune misure di attenuazione nel rispetto dei diritti fondamentali. Nel determinare la rilevanza dei potenziali effetti e impatti negativi, i fornitori dovrebbero considerare la gravità dell'impatto potenziale e la probabilità di tutti questi rischi sistemici. Ad esempio, potrebbero valutare se il potenziale impatto negativo possa incidere su un gran numero di persone, la sua potenziale irreversibilità o la difficoltà nel porvi rimedio e ripristinare la situazione esistente prima dell'impatto potenziale".
68. In particolare, cfr. art. 34, par. 1, lett. b) e c), ove si impone la valutazione del rischio alle grandi piattaforme e motori di ricerca per "eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta" e "eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica".

Il *Media Freedom Act*[69] e l'atto normativo che più direttamente impatta il regime dei servizi media, con specifica finalizzazione alla tutela del pluralismo: di particolare rilievo l'art. 18 del Regolamento che introduce una specifica e dettagliata disciplina sui contenuti di fornitori di servizi di media su piattaforme online di dimensioni molto grandi.

Tutte le disposizioni normative sin qui citate si basano sull'art. 114 TFUE[70], cioè – come puntualmente, e in parte criticamente, rilevato[71] – sul ravvicinamento delle disposizioni degli Stati membri per il funzionamento del mercato unico. Una base giuridica non particolarmente solida, eppure così intensamente utilizzata per adottare corpi normativi vasti e di grande impatto.

Non così il Regolamento sul targeting politico[72] che invece si base anche – come il GDPR – sull'art. 16 TFUE e cioè sulla competenza dell'Ue in tema di disciplina della protezione dei dati personali.

Forse è sufficiente mettere a confronto il contenuto della l. n. 28/00 con quello del Reg. 2024/900 relativo alla *trasparenza e al targeting della pubblicità politica* per comprendere buona parte di quanto sin qui si è inteso affermare in merito all'evoluzione del significato del principio del pluralismo informativo: si disciplina il targeting politico per "tutelare i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla vita privata e la protezione dei dati personali" (art. 1, par. 4, lett. b). Come ben si può comprendere il confine fra contenuti sponsorizzati (e quindi pubblicitari) e comunicazione di altra natura, sarà forse uno dei campi di maggior interesse nella applicazione del Regolamento[73], e che si presta ad offrire importanti spunti per la determinazione operativa del principio pluralista.

7. Il pluralismo di fronte ai rischi sistemici. Sicurezza cibernetica e IA generativa. Guerra e realtà ibrida

Un tempo sembrava una sottolineatura in parte enfatica o retorica affermare "il valore centrale del pluralismo in un ordinamento democratico" (Corte cost., sent. 826/1988). In realtà, l'affermazione oggi appare tutt'altro che retorica, se si osserva la portata dei cd. "rischi sistemici": al punto di confluenza fra DSA e Reg. sul targeting politico si collocano dei nuovi Orientamenti della Commissione per i rischi sistemici[74] per i processi elettorali (*ex* art. 35, par. 3, DSA).

Si tratta di un documento di indirizzo, rivolto alle piattaforme ed ai motori di ricerca molto grandi, che meriterebbe un approfondimento a sé stante. Ha il grande pregio di mettere a terra l'insieme dei temi che coinvolgono il principio del pluralismo rovesciato, nel contenitore delle Misure specifiche di attenuazione dei rischi per le elezioni (par. 3). D'altra parte, come più volte osservato in questo contributo, è evidente anche in questo caso una certa confusione e commistione di tematiche sotto il grande cielo della disciplina europea del pluralismo e soprattutto sotto la grande pressione di doversi difendere da pericoli che ancora non sono né chiari né pienamente prevedibili.

Quindi – senza nessuna pretesa di completezza – vi sono indicazioni in merito a:

- par. 3.1 "rafforzamento dei processi interni" che implica una attenzione anche per i rischi del contesto territoriale e locale del singolo Stato membro; l'esigenza di valersi di analisi indipendenti (come quella espressamente citata del Media pluralism monitor[75]; l'istituzione di una squadra interna dedicata e identificabile alle singole tornate elettorali; la modifica delle

69. Reg. (UE) 2024/1083 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media).
70. Cfr. Longo 2025.
71. Cfr. Donati 2024, p. 243.
72. Reg. (UE) 2024/900 relativo alla trasparenza e al targeting della pubblicità politica.
73. Lobascio 2025.
74. Comunicazione della Commissione (C/2024/3014), "Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del regolamento (UE) 2022/2065".
75. … curato dal Center for Media Pluralism and Media Freedom, coordinato attualmente da Elda Brogi, con sede presso l'European University Institut di Firenze, che cura fra l'altro il modello cui si conforma il Monitor e,

condizioni generali con specifico riferimento alle misure specifiche dedicate al periodo elettorale; adottare misure specifiche in precedenza rispetto al periodo elettorale ed in seguito al medesimo;
– 3.2 Misure di attenuazione dei rischi per i processi elettorali, distinte in misure di attenuazione specifiche (par. 3.2.1[76]), misure di controllo, ricerca e accesso ai dati da parte di terzi (par. 3.2.2), diritti fondamentali (par. 3.2.3);
– 3.3 Misure di attenuazione legate all'IA generativa[77].

Inoltre, oltre alla cooperazione con autorità nazionali, esperti e associazioni, vi sono indicazioni in merito al periodo elettorale (in particolare, sulla gestione di eventuali incidenti[78] secondo

su tale base, la redazione di rapporti sul pluralismo per ciascuno Stato membro (o candidato tale). Cfr. MPM, *Mapping risks for media pluralism and the safety of journalists across Europe*; per l'Italia: Vigevani–Mazzoleni–Canzian–Cecili 2024.

76. Qui vi è un primo elenco di misure, se si osserva bene pressoché tutte volte a tutelare la libertà cognitiva e la libera formazione del pensiero dell'utente: a) Accesso alle informazioni ufficiali sul processo elettorale; b) Iniziative di alfabetizzazione mediatica; c) Misure tese a fornire agli utenti informazioni più contestuali sui contenuti e sugli account con cui interagiscono, in particolare attraverso "i. etichette di verifica dei fatti sui contenuti identificati di disinformazione e manipolazione delle informazioni e ingerenze da parte di attori stranieri, fornite da verificatori di fatti e squadre di verifica dei fatti indipendenti che appartengano a organizzazioni mediatiche indipendenti. La verifica dei fatti dovrebbe estendersi a tutta l'UE e a tutte le lingue dell'Unione, anche rafforzando la cooperazione con i verificatori di fatti locali durante i periodi elettorali, integrando e presentando contenuti di verifica dei fatti relativi alle elezioni e utilizzando meccanismi per contribuire ad accrescerne l'impatto sul pubblico. Le etichette di verifica dei fatti dovrebbero essere accessibili e scritte in un linguaggio facilmente comprensibile; ii. esortazioni e suggerimenti che spingano gli utenti a leggere i contenuti e a valutarne l'accuratezza e la fonte prima di condividerli; iii. indicazioni chiare, visibili e non ingannevoli di account ufficiali, nonché di account che forniscano informazioni autorevoli sul processo elettorale, come gli account delle autorità elettorali, compresa la base su cui si fonda tale verifica. I criteri utilizzati per concedere un'etichetta "ufficiale" a un account dovrebbero essere accessibili e illustrati in un linguaggio facilmente comprensibile, per evitare che tali indicazioni conferiscano credibilità ad account che si presentano come account ufficiali, ad esempio delle autorità elettorali; iv. etichettatura chiara, visibile e non ingannevole degli account controllati da Stati membri, paesi terzi ed entità controllate o finanziate da entità a loro volta controllate da paesi terzi; v. strumenti e informazioni tesi ad aiutare gli utenti a valutare l'affidabilità delle fonti di informazione, come i marchi di fiducia per l'integrità della fonte basati su metodologie trasparenti e sviluppati da terzi indipendenti; vi. altri strumenti utilizzabili per valutare la provenienza, la cronologia delle modifiche, l'autenticità o l'accuratezza del contenuto digitale, che aiutano gli utenti a verificare l'autenticità o a identificare la provenienza o l'origine dei contenuti relativi alle elezioni; vii. misure interne efficaci per contrastare l'uso improprio delle procedure e degli strumenti di cui sopra, e in particolare l'abuso del processo di verifica per gli account e i contenuti etichettati"; d) sistemi di raccomandazione; e) pubblicità politica; f) gli influencer; g) Demonetizzazione dei contenuti di disinformazione; e) Integrità dei servizi.
77. Anche queste misure appaiono di grande rilievo: i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi devono valutare i rischi sistemici fra cui quelli derivanti dall'utilizzo dell'IA generativa, cui è richiesto l'utilizzo di filigrane elettroniche (watermark), la produzione di informazioni attendibili, la segnalazione di errori e il rinvio alla consultazione di fonti autorevoli, test di red teaming, il monitoraggio continuo, lo sviluppo di pratiche di sicurezza, il rinvio alle fonti delle informazioni su cui si basano gli output.
78. L'incidente è la conseguenza dell'avverarsi di una minaccia: "La disinformazione, la manipolazione delle informazioni e le ingerenze da parte di attori stranieri costituiscono una grave minaccia per la nostra società. Infatti possono compromettere le istituzioni e i processi democratici (come le elezioni) impedendo ai cittadini di prendere decisioni informate o spingendoli a non votare. Inoltre possono polarizzare le società creando conflitti fra le comunità". Cfr. Commissione europea, *Comunicazione strategica e lotta alla manipolazione delle informazioni*

il metodo del "seguire il sole", cfr. par. n. 57) e al periodo post-elettorale (attraverso appositi riesami dell'esperienza maturata).

I temi della gestione degli incidenti in periodo elettorale e delle misure di attenuazione legate all'IA generativa, ci introducono agli ultimi due aspetti coinvolti nell'assetto attuale del principio del pluralismo[79].

Ovvero i nessi fra principio del pluralismo e sicurezza cibernetica[80], da un lato, e gli aspetti connessi con l'avvento della realtà ibrida (IA[81] e contenuti sintetici): si tratta di nuovi volti della disinformazione, di un nuovo assetto della realtà e della guerra (ibride[82]). Questi due temi coinvolgono specificamente l'assetto democratico-costituzionale dello Stato, o se si preferisce costituiscono rischi specifici – e vulnerabilità proprie – degli ordinamenti democratici, a differenza di altre forme di Stato, segnatamente di quelle autoritarie o a tendenza autoritaria, e la tutela del principio del pluralismo rappresenta davvero un rimedio giuridicamente apprezzabile e genuinamente liberaldemocratico per affrontare questi pericoli concreti.

Non è possibile ripercorrere qui come il profilo della sicurezza cibernetica rappresenti ormai un aspetto centrale della sicurezza (anche strettamente militare) dello Stato[83], ma ormai l'esperienza oltre a numerosi atti giuridici di varia natura ed alla stessa strategia della NATO[84], documentano che la disinformazione è «un'arma» e che è stata utilizzata per indirizzare, destabilizzare, distruggere le realtà, anche ordinamentali, che sono prese di mira. Questa arma si avvale di software e di bot, di account fittizi, di deep-fake, della dinamica comunicativa, immersiva e informativa dei social, della rapida polarizzazione e dell'emotività eccessiva indotta dalla connessione ininterrotta e ossessiva, insomma di tutto l'armamentario che la comunicazione e l'informazione digitale mette a disposizione di agenti malevoli.

L'avvento dell'intelligenza artificiale generativa – che produce essenzialmente contenuti sintetici[85] – è davvero un fattore che deve destare nelle persone mediamente avvedute una grande preoccupazione, come peraltro ha già profondamente preoccupato un legislatore normalmente riottoso ad introdurre discipline che potrebbero ostacolare la supremazia tecnologica come quello statunitense[86]: si tratta infatti di contenuti prodotti e messi in circolazione nello spazio digitale senza che, attualmente, gli esseri umani possano distinguerli dai contenuti non sintetici – cioè dai contenuti aventi una origine effettivamente umana.

Ciò significa che il famoso *market place of ideas* attualmente può essere simulato, influenzato, indirizzato, manomesso, attraverso l'immissione di contenuti (invisibilmente) sintetici.

---

e alle ingerenze da parte di attori stranieri e più specificamente European Commission, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence*, January 2024.

79. Cfr. Pollicino–Dunn 2024, p. IV ss.

80. Longo 2024, p. 203 ss.; Di Corinto 2023.

81. Reg. (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

82. Si veda su questo aspetto Cossiri 2023, p. 77 ss.; Spaziani 2024.

83. Ma v. Martino 2018, p. 61 ss.

84. Cfr. Spaziani 2024, spec. p. 519 ss.

85. Si tratta di contenuti originali, autentici, prodotti in tutto o in parte significativa dall'IA generativa, ma non di origine umana. Cfr. sul tema, nella prospettiva di una nuova vulnerabilità della democrazia, Calzolaio 2023-b, p. 14 ss., spec. p. 24 ss.

86. U.S. Executive Order 14110, October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.* Il 20 gennaio 2025 il Presidente Trump ha revocato – con apposito *executive order* – numerosi provvedimenti del precedente Presidente Biden, fra cui proprio il n. 14410/2023. Ha peraltro adottatto, successivamente (23 gennaio 2025), un apposito *executive order* denominato *Removing barriers to american leadership in artificial intelligence*, rivolto a porre una nuova disciplina in materia, orientata alla deregolazione e alla attrazione di investimenti per garantire e ampliare la supremazia degli USA in materia.

È bene aver presente che i contenuti sintetici sono utili, sotto molteplici profili (fra cui l'addestramento di sistemi di IA attraverso dati, appunto, sintetici), e inoltre sono qui per restare: la nostra realtà, segnatamente quel vecchio concetto di sistema dell'informazione, è già radicalmente ibridato da contenuti sintetici, cioè da contenuti dall'apparente origine umana e non distinguibili dai contenuti di origine umana, ma non umani (che superano facilmente il test di Touring[87]!). La nostra è una realtà ibrida, in cui quindi la dimensione cibernetica della sicurezza, la nozione di disinformazione e la nozione di guerra ibrida sono concetti e dinamiche strutturali.

Questi profili sono il campo d'azione e di sviluppo per il "nostro" principio del pluralismo rovesciato, che implicano l'invenzione di nuove dimensioni regolatorie che ne tengano conto specificamente[88] e di aver chiaro che l'obiettivo finale, in un ordinamento democratico-costituzionale, è tutelare la libertà individuale di formazione del pensiero nel contesto ibrido.

In questo ambito, il pluralismo rovesciato avrà facilmente bisogno di svilupparsi per il tramite della tecnologia e di strumenti di intelligenza artificiale che tutelino la cd. *diversity by design* e *by default*.

8. *Overload* normativo e *overload* istituzionale. Elogio del costituzionalismo e contro la burocrazia dell'informazione

Si afferma comunemente che il PPI è messo a rischio dagli *Over the Top*, dalle piattaforme e dai motori di ricerca di dimensioni molto grandi di cui al DSA, che poi sono essenzialmente le arcinote grandi aziende americane della tecnologia digitale[89].

Si condivide la preoccupazione, ma con una osservazione che mi è capitato – studiando – di dover fare e che mi fa sottolineare un aspetto sostanziale controtendenza[90].

L'Unione europea ha adottato e sta adottando in materia digitale un numero davvero significativo di norme e in un lasso temporale davvero ridotto. È una osservazione che circola – peraltro carica di una molteplicità di implicazioni[91].

Leggendo le numerose discipline europee in materia, alcune delle quali abbiamo passato in rassegna, si può osservare una costante: una concentrazione inedita di potere di programmazione e di indirizzo, di spesa, di verifica e di controllo anche (e soprattutto) tecnico, oltreché di normazione tecnica e attuativa, in capo ad un unico soggetto. La Commissione europea.

Non si può approfondire il tema qui: ma parafrasando Sabino Cassese[92], si può osservare che le Big Tech passano (con l'evolversi del mercato), mentre l'assetto dei poteri pubblici resta e, in questo caso, può non essere un fattore positivo per il pluralismo informativo e per la libertà di espressione in genere.

Come si è osservato, all'*overload informativo* l'Unione europea ha reagito con un frenetico *overload normativo*[93], da cui a guardar bene emerge un *overload istituzionale* (di potere della Commissione europea).

Il principio del pluralismo – nella sua dimensione più genuinamente tradizionale – ci insegna che, storicamente, la libertà di espressione si è affermata in primo luogo nei confronti dei poteri pubblici, di cui non ama e non accetta la

87. Turing 1950, pp. 433-460.

88. … ad es.: la difesa del perimetro cibernetico dello Stato è rivolta, e deve esserlo anche normativamente, non solo a resistere ed a respingere gli attacchi informatici che si sviluppano per il tramite della disinformazione, ma proprio a promuovere il principio del pluralismo, in forza del quale tutte le opinioni (reali) hanno diritto di essere rappresentate e nessuna ha diritto ad essere sovra o sottorappresentata artificiosamente.

89. Sul tema, acutamente, Niro 2023, p. 255 ss.

90. Cfr. Calzolaio 2024, p. 83 ss., e più di recente, Calzolaio 2025, p. 139 ss.

91. … prima fra tutte che questa mole di norme europee appare una forma di reazione impulsiva più rivolta a rassicurare di fronte al timore di qualsiasi rischio, che ad affrontarli in modo appropriato ed ordinato.

92. Cassese 2002, p. 1341.

93. … che sembra non trovare alcun momento di autoriflessione in merito ai benefici di continui e massivi interventi normativi, rispetto – talvolta – ai benefici di interventi normativi limitati o di nessun intervento normativo.

pervasività e l'onnipresenza in tutti gli ambiti della vita sociale, che deve essere libera anche dall'influenza del governo (nazionale o europeo): "la libertà di pensiero nasce e si consolida, non a caso, proprio come libertà fondamentale del singolo "contro" il potere pubblico; e questa impostazione, che circonda di cautele l'intervento pubblico nel mercato dell'informazione ed è ostile a ogni forma di controllo pubblico sulla qualità e la direzione dei flussi informativi, è quella ancora oggi scolpita nelle costituzioni delle democrazie liberali, fra cui certamente anche quella italiana. E già questo dovrebbe portare a guardare con sospetto le più recenti tendenze che oggi vorrebbero restituire un qualche ruolo alla mano pubblica nella selezione dei contenuti informativi"[94].

Anche questo è un punto di lavoro da non sottovalutare: la dimensione del principio del pluralismo negli ordinamenti democratici europei di fronte al sorgere di grandi apparati burocratici pubblici, spesso sotto il controllo diretto dell'esecutivo nazionale o europeo[95], sorti per contrastare l'effettivo potere dei grandi OTT.

Per dirla ancora con Vigevani: "ciò che desta maggiore preoccupazione non è la privatizzazione del controllo sui contenuti tout court, quanto il sistema di controllo sui c.d. "poteri privati" escogitato dai poteri pubblici"[96].

9. Vulnerabilità e vivacità dell'ordinamento costituzionale della politicità e dell'informazione (Corte cost. sent. n. 44/2025)

Nei momenti di evoluzione e rivoluzione tecnologica non è possibile fermare il vagone del treno, scendere, e osservare quel che succede. In realtà, non è mai possibile.

Pertanto, dopo aver cercato di descrivere il più accuratamente possibile la nuova sfida del (vecchio) PPI, si può solo concludere osservando che quanto descritto rappresenta un quadro di nuove vulnerabilità dell'ordinamento costituzionale.

Il principio del pluralismo – l'affronto del tema – aiuta ad osservare che quel che è in discussione, in questa fase, è proprio la dimensione politica, ultra-individuale, delle società contemporanee[97].

Vi sono nessi, pertanto, fra vulnerabilità delle democrazie e tutela del pluralismo, così come fra esigenze pluraliste e dimensione politica della società. Gli ordinamenti costituzionali liberaldemocratici contemporanei si confermano come ordinamenti in cui la principale vulnerabilità risiede nell'incapacità di mantenere e rinvigorire una effettiva e vivace dimensione della politicità dell'essere umano, che invece era familiare agli estensori, ed ai commentatori, della Costituzione italiana e segnatamente presente nell'art. 2 della stessa[98]. Il pluralismo rovesciato non ribalta l'ordine costituzionale, anzi lo invoca così come tradizionalmente ci è stato consegnato. Appare anzi utile a scoprire di nuovo (ri-scoprire) la novità impressa nella

94. Vigevani 2025, pp. 243-244. Prosegue l'A. affermando che "Non va però al contempo dimenticata la complessità della dinamica storica che si è appena evocata, in cui gli apparati burocratici censori (che certamente ci appaiono, visti oggi, odiosi) rispondevano anche a esigenze emerse dalle stesse società su cui insistevano, per assicurare le condizioni minime della convivenza pacifica all'interno di comunità in cui la coesione religiosa (e quindi anche di pensiero) era un requisito irrinunciabile. Né può essere trascurato il fatto che i sistemi di controllo istituiti per motivi religiosi e gestiti dalle autorità ecclesiastiche si siano anche rivelati utili strumenti di governo sociale pure nella prospettiva dei detentori del potere politico. Con ciò non si vuole certo celebrare l'affermazione della censura nell'Europa moderna, ma ricordare come essa si sia sviluppata nel momento in cui un'evoluzione tecnologica dirompente si è verificata in un contesto non attrezzato a gestirne tutte le conseguenze; e che dunque non è nemmeno nuovo il fenomeno per cui la richiesta di forme di controllo anche preventivo vengono da settori della società, e con le migliori intenzioni, magari accompagnate da una certa sfiducia sulla capacità delle masse di reggere con serenità l'urto di nuovi mezzi di comunicazione".

95. Cfr. Calzolaio 2024, p. 83 ss.

96. *Ivi*, p. 256.

97. Giacomini–Buriani 2022; Giacomini 2018.

98. Cfr. Barbera 1975.

tradizione costituzionale italiana e a riaccendere la consapevolezza di poter affrontare la società digitale con i principi ivi impressi e sviluppati.

E non a caso – proprio mentre si licenzia questo contributo – soccorre all'interprete l'indirizzo della Corte costituzionale italiana che sembra avvedersi dell'esistenza del principio del pluralismo rovesciato e apre i classici istituti del costituzionalismo italiano alle sfide della società digitale.

Nella sent. n. 44/2025[99] – che sicuramente merita più attenta analisi – afferma che "l'«ecosistema» dell'informazione è radicalmente mutato, risultando ora caratterizzato, a qualsiasi livello (locale, nazionale e globale), sia dall'eliminazione delle barriere di ordine tecnico alla moltiplicazione dei produttori e distributori di informazione sia dalla diminuzione dei costi economici inerenti a tali attività. Soprattutto, per l'intero ecosistema vale il rilievo che la quantità di informazioni e di differenti punti di vista disponibili si è accresciuta enormemente grazie ad internet, che ha assunto un ruolo centrale, come analiticamente illustrato nel diciannovesimo Rapporto sulla comunicazione («Il vero e il falso») del Centro studi investimenti sociali (CENSIS), dell'11 marzo 2024".

Osserva poi – in modo davvero innovativo rispetto alla configurazione del PPI – che "le trasformazioni sinteticamente richiamate plasmano l'attuale significato del pluralismo dell'informazione, a qualsiasi livello, e, conseguentemente, la declinazione delle concrete modalità della sua tutela, che sono sempre state, nella giurisprudenza di questa Corte, raccordate allo specifico contesto in cui l'informazione si situava. La ricordata ricchezza di informazioni e di punti di vista alternativi, anche di quelli particolarmente eterodossi rispetto alle idee maggioritarie e critici nei confronti dell'establishment, cui ha accesso l'utente, grazie a Internet, si accompagna a una crisi di *qualità dell'informazione* [nostro il corsivo]. È noto, infatti, che, soprattutto in assenza dei controlli editoriali che caratterizzano l'operato dei media tradizionali, sulla rete si diffondono informazioni false, discorsi d'odio, affermazioni non verificate e opinioni polarizzate. In definitiva, l'attuale sfida dell'informazione non riguarda tanto la ulteriore moltiplicazione delle già numerose voci che si fanno sentire nella sfera pubblica, quanto la salvaguardia della qualità dell'informazione medesima. Tale esigenza appare tanto più pregnante ove si consideri che il pluralismo dell'informazione – tutelato dall'art. 21 Cost., dall'art. 11 CDFUE e dall'art. 10 CEDU – va riguardato non solo nella prospettiva del diritto di informare, ma anche in quella del diritto di ricevere l'informazione, ossia nella prospettiva dei cittadini che devono essere posti nella condizione di accedere a diversi punti di vista, per formarsi un'opinione con cui potere, tra l'altro, esercitare consapevolmente i diritti di partecipazione politica. Affinché sia tutelato questo diritto, in un ambiente in cui sono prodotte e distribuite quantità enormi di informazioni, che espongono il cittadino a un vero e proprio sovraccarico mediatico, occorre tutelare e promuovere la qualità della comunicazione.

Quest'ultima, anche e soprattutto nei media tradizionali, di cui in questa sede si discute, può essere assicurata dando risalto alla funzione dei giornalisti operanti entro strutture dotate di una consistenza organizzativa e tecnologica tale da permettere il vaglio critico delle notizie, le inchieste e le analisi".

Siamo ufficialmente entrati nell'era del principio del pluralismo rovesciato. E il nostro ordinamento costituzionale mostra la vivacità necessaria per affrontarla.

Riferimenti bibliografici

AGCOM (2023), *Segnalazione al Governo ai sensi dell'articolo 1, comma 6, lettera c), n. 1 della legge 31 luglio 1997, n. 249 per la revisione della normativa in materia di comunicazione politica e di accesso ai mezzi di informazione*, 28 luglio 2023

M.R. Allegri (2020), *Oltre la par condicio. Comunicazione politico-elettorale nei social media, fra diritto e autodisciplina*, Franco Angeli, 2020

99. … su cui Paolanti 2025.

E. Apa (2021), *Sic et non: nel caso Vivendi la Corte di giustizia censura le incongruenze della disciplina italiana a tutela del pluralismo dell'informazione*, in "Medialaws", 2021, n. 1

A. Barbera (1975), *Articolo 2 Cost.*, in G. Branca (a cura di), "Commentario della Costituzione. Artt. 1-12. Principi fondamentali", Zanichelli, 1975

F. Battaglia (a cura di) (1962), *Antologia degli scritti politici di John Locke*, il Mulino, 1962

D. Bawden, L. Robinson (2020), *Information Overload: An Overview, in Oxford Encyclopedia of Political Decision Making*, Oxford University Press, 2020

F. Biondi Dal Monte (2018), *Esiste ancora la "par condicio"? Contenuto e limiti della legge n. 28/2000*, in "Osservatorio costituzionale", 2018, n. 1

N. Bobbio (2004), voce *Pluralismo*, in N. Bobbio, N. Matteucci, G. Pasquino "Il dizionario di politica", UTET, 2004

R. Borrello (2019), *Due profili di riflessione sulla disciplina della comunicazione politica*, in M. Manetti, R. Borrello (a cura di), "Il diritto dell'informazione. Temi e problemi", Mucchi editore, 2019

R. Borrello (2017), *Alcune riflessioni preliminari (e provvisorie) sui rapporti tra i motori di ricerca ed il pluralismo informativo*, in "Medialaws", 2017, n. 1

C. Calvieri (a cura di) (2025), *La riforma della* par condicio. *Pluralismo sui nuovi media. Le garanzie per il cittadino. Atti di Convegno - Perugia, 15 dicembre 2023*, Giappichelli, 2025

S. Calzolaio (2025), *Autorità, governo, attuazione dell'AI Act*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, "La regolazione europea dell'intelligenza artificiale nella società digitale", Giappichelli, 2025

S. Calzolaio (2025-a), *Il pluralismo rovesciato. Pluralismo e par condicio al tempo dell'infosfera*, in C. Calvieri (a cura di), "La riforma della *par condicio*. Pluralismo sui nuovi media. Le garanzie per il cittadino. Atti di Convegno - Perugia, 15 dicembre 2023", Giappichelli, 2025

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, "La regolazione europea della società digitale", Giappichelli, 2024

S. Calzolaio (2023), *Isolamento e relazioni sociali. Il Connection-in-All-Policies approach, Nota a: U.S. Surgeon General (2023), Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community, 2023*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2023-a), *Social media e minori. Il Safety-first approach, Nota a: U.S. Surgeon General, Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory, 2023*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2023-b), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2018), *Recensione a: "Neil Richards, Intellectual privacy. Rethinking civil liberties in the digital age, Oxford University Press, 2015"*, in "Giornale di storia costituzionale", 2018, n. 36

S. Calzolaio (2017), voce *Protezione dei dati personali*, in "Digesto delle discipline pubblicistiche", UTET, 2017

S. Calzolaio (2008), *Il sistema dell'informazione tra Unione europea e legislazione interna*, in "forumcostituzionale.it", 4 maggio 2008

B. Caravita di Toritto (2023), *Social network, formazione del consenso, istituzioni politiche: quale regolamentazione possibile?*, in A. Poggi, F. Fabrizzi, F. Savastano (a cura di), "Social Network, formazione

del consenso, intelligenza artificiale. Itinerario di un percorso di ricerca di Beniamino Caravita", Sapienza Università Editrice, 2023

P. Caretti, A. Cardone (2024), *Il diritto dell'informazione e della comunicazione nell'era dell'intelligenza artificiale*, il Mulino, 2024

C. Caruso (2013), *La libertà di espressione in azione. Contributo a una teoria costituzionale del discorso pubblico*, Bononia University Press, 2013

S. Cassese (2002), *Il nuovo regime dei dirigenti pubblici italiani: una modificazione costituzionale*, in "Giornale di diritto amministrativo", 2002, n. 12

CENSIS (2023), *Il vero e il falso*, 19° Rapporto sulla comunicazione, 2023

A. Collins (1713/2019), *Discorso sul libero pensiero*, Liberilibri, 2019

A. Cossiri (2023), *Le campagne di disinformazione nell'arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento*, in "Rivista italiana di informatica e diritto", 2023, n. 2

M. Cuniberti (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in "Medialaws", 2017, n. 1

A. Di Corinto (2023), *Netwar, come cambia l'hacktivismo nella guerra cibernetica*, in "Rivista italiana di informatica e diritto", 2023, n. 2

G. Di Cosimo (a cura di) (2023), *Processi democratici e tecnologie digitali*, Giappichelli, 2023

F. Donati (2024), *Antitrust, pluralismo e regolazione delle piattaforme dopo il Digital service Act e il Media Freedom Act*, in "Lo Stato", 2024, n. 22

F. Donati (2019), *Internet e campagne elettorali*, in "federalismi.it", 2019, n. 16

F. Donati (2018), *L'art. 21 della Costituzione settanta anni dopo*, in "Rivista di diritto dei media", 2018, n. 1

L. Floridi (2014), *The fourth revolution: How the infosphere is reshaping human reality*, Oxford University Press, 2014

G. Gardini (2021), *Le regole dell'informazione. Verso la Gigabit Society*, Giappichelli, 2021

G. Gardini (2015), *RAI e servizio pubblico radiotelevisivo: la "cultura italiana" in bilico tra unità, pluralismo e mercato*, in "Munus", 2015, n. 2

G. Giacomini (2018), *Potere digitale. Come Internet sta cambiando la sfera pubblica e la democrazia*, Meltemi, 2018

G. Giacomini, A. Buriani (2022), *Il governo delle piattaforme. I media digitali visti dagli italiani*, Meltemi, 2022

O. Grandinetti (2022), *La tutela del pluralismo nel nuovo Testo unico dei media audiovisivi*, in "Medialaws", 2022, n. 2

O. Grandinetti (2019), *La par condicio nei programmi di informazione: alcuni sviluppi recenti*, in M. Manetti, R. Borrello (a cura di), "Il diritto dell'informazione. Temi e problemi", Mucchi editore, 2019

O. Grandinetti (2002), *"Par condicio", pluralismo e sistema televisivo, tra conferme e novità giurisprudenziali, in un quadro comunitario tecnologico in evoluzione*, in "Giurisprudenza costituzionale", 2002, n. 3

Y.N. Harari (2016), *Homo Deus: A Brief History of Tomorrow*, HarperCollins, 2016

A. Italia (2024), *La televisione nella società connessa*, in "Note e commenti – Tante verità", 2024, n. 796

C. Lobascio (2025), *Micro-targeting politico e protezione dei dati personali. Il Regolamento (UE) 2024/900*, in "Rivista italiana di informatica e diritto", 2025, n. 1

E. Longo (2025), *Grounding media freedom in the EU: The legal basis of the EMFA*, in "Rivista italiana di informatica e diritto", 2025, n. 1

E. Longo (2024), *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, "La regolazione europea della società digitale", Giappichelli, 2024

M. Luciani (2023), *La Costituzione e il pluralismo*, in P. Cappellini, G. Cazzetta (a cura di), "Pluralismo giuridico. Itinerari contemporanei. Firenze 20-21 ottobre 2022", Giuffrè, 2023

M. Manetti (2012), *Pluralismo dell'informazione e libertà di scelta*, in "Rivista AIC", 2012, n. 1

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "il Mulino", 2018, n. 1

A. Martusciello (2019), *Le iniziative AGCOM in materia di pluralismo e di correttezza dell'informazione sulle piattaforme digitali*, in M. Manetti, R. Borrello (a cura di), "Il diritto dell'informazione. Temi e problemi", Mucchi editore, 2019

N. Matteucci (2001), *Pluralismo*, in "il Mulino", 2001, n. 3

F. Meola (2020), *Tecnologie digitali e* neuro-marketing *elettorale. A proposito di una possibile regolamentazione delle nuove forme di propaganda politica*, in "Costituzionalismo.it", 2020, n. 1

R. Montaldo (2020), *La tutela del pluralismo informativo nelle piattaforme online*, in "Rivista di diritto dei media", 2020, n. 1

A. Napolitano (2020), *L'evoluzione del sostegno economico alla stampa tra tutela del pluralismo informativo ed esigenze di razionalizzazione della spesa*, in "federalismi.it", 2020, n. 30

R. Niro (2023), *Piattaforme digitali e libertà di espressione fra auto-regolamentazione e co-regolazione: note ricostruttive*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

G. Origgi (2018), *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in "Ragion Pratica", 2018

M. Orofino (2024), *Il Digital service act tra continuità (solo apparente) ed innovazione*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, "La regolazione europea della società digitale", Giappichelli, 2024

M. Orofino (2020), *SIC… transit gloria mundi. La Corte di giustizia dichiara le soglie asimmetriche del sistema integrato delle comunicazioni incompatibili con la libertà di stabilimento*, in "Osservatorio costituzionale", 2020, n. 6

A. Pace, M. Manetti (2006), *La libertà di manifestazione del proprio pensiero*, in G. Branca, A. Pizzorusso (a cura di), "Commentario della Costituzione", Zanichelli, 2006

V. Pampanin (2019), *Strumenti di regolazione a garanzia del mercato pluralistico dell'informazione online*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2019

M. Paolanti (2025), *La sentenza n. 44/2025 della Corte costituzionale: implicazioni per il pluralismo informativo e il diritto alla concorrenza*, in "Consulta Online", 2025, n. 2

G. Pavani (2016), *La governance dei sistemi radiotelevisivi pubblici: una questione culturale,* in "federalismi.it", 2016, n. 1

G. Pavani (2012), *Radiotelevisioni. Profili storici e comparati*, Filo diritto, 2012

G. Pitruzzella (2017), *La libertà di informazione nell'era di Internet*, in "Medialaws", 2018, n. 1

O. Pollicino, P. Dunn (2024), *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in "federalismi.it", 2024, n. 12

N. Richards (2015), *Intellectual Privacy. Rethinking civil liberties in the digital age*, Oxford University Press, 2015

F. Rosa (2025), *L'annullamento delle elezioni presidenziali in Romania e la difficile difesa della democrazia*, in "federalismi.it", 2025, n. 15

M. Rubechi (2016), *Il diritto di voto. Profili costituzionali e prospettive evolutive*, Giappichelli, 2016

V. Salvatore (1993), *Concorrenza televisiva e diritto comunitario*, CEDAM, 1993

A. Spaziani (2024), *L'attacco cibernetico nell'era della guerra ibrida*, in "DPCE Online", 2024, n. sp1

C.R. Sunstein (2021), *Liars. Falsehoods and Free Speech in an Age of Deception*, Oxford University Press, 2021

A.M. Turing (1950), *Computing Machinery and Intelligence*, in "Mind", 1950, n. 49

G.E. Vigevani (2025), *Potere politico e mezzi di comunicazione*, in "Rivista AIC", 2025, n. 2

G.E. Vigevani, M. Cazzaniga (2024), *Comunicazione politica e Costituzione tra televisione e piattaforme digitali*, in "Medialaws", 2024, n. 1

G.E. Vigevani, G. Mazzoleni, N. Canzian, M. Cecili (2024), *Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023. Country report: Italy*, EUI, RSC, Research Project Report; Centre for Media Pluralism and Media Freedom (CMPF), 2024

Y. Wang, M. McKee, A. Torbica, D. Stuckler (2019), *Systematic literature review on the spread of health-related misinformation on social media*, in "Social Science & Medicine", vol. 240, 2019

C. Wardle, H. Derakhshan (2017), *Information Disorder. Toward an interdisciplinary framework for research and policymaking*, Council of Europe report DGI(2017)09, 2017

R. Zaccaria, A. Valastro, A. Albanesi (2023), *Diritto dell'informazione e della comunicazione*, CEDAM, 2023

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0209 • articolo sottoposto a peer review • pubblicato in anteprima il 10 feb. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Erik Longo

Grounding media freedom in the EU: The legal basis of the EMFA

The article critically examines the choice of Article 114 TFEU as the legal basis for the European Media Freedom Act (EMFA), which aims to harmonise media regulation across Member States to support media freedom and pluralism. The study, firstly, identifies two contrasting perspectives (critics and supporters of the chosen legal basis) and, secondly, highlights two shortcomings of the EMFA (its focus on market-based solutions risks commodifying freedom of expression and its ex-ante regulatory framework). Despite these concerns, the author argues that the EMFA represents a constitutional evolution for the EU, bridging old and new media paradigms to ensure democratic values and the integrity of the digital market. The conclusion argues that the broad interpretation of Article 114 TFEU is justified and in line with the EU's role in safeguarding democracy and fundamental rights and signalling the new direction of EU integration. However, the success of the EMFA will depend on its effective implementation and the capacity of EU institutions to ensure freedom of expression, fair competition and robust regulation in the digital age.

EMFA – Media Pluralism – Media Freedom – Harmonisation – Legal Basis

Il fondamento della libertà dei media nell'UE: la base giuridica dell'EMFA

L'articolo esamina criticamente la scelta dell'articolo 114 del TFUE come base giuridica dell'*European Media Freedom Act* (EMFA), che mira ad armonizzare la regolamentazione dei media tra gli Stati membri per sostenere la libertà e il pluralismo dei media. Lo studio identifica due prospettive contrastanti (critici e sostenitori della base giuridica scelta) e mette in evidenza due difetti dell'EMFA (il suo focus sulle soluzioni basate sul mercato rischia di mercificare la libertà di espressione e il suo quadro normativo *ex-ante* può mancare di precisione). Nonostante queste preoccupazioni, l'autore sostiene che l'EMFA rappresenta un'evoluzione costituzionale per l'UE, che collega i paradigmi dei vecchi e dei nuovi media per garantire i valori democratici e l'integrità del mercato digitale. La conclusione sostiene che l'interpretazione ampia dell'Articolo 114 del TFUE è giustificata e in linea con il ruolo dell'UE nella salvaguardia della democrazia e dei diritti fondamentali, oltre a segnalare la nuova direzione dell'integrazione dell'UE. Tuttavia, il successo dell'EMFA dipenderà dalla sua effettiva attuazione, garantendo la libertà di espressione, la concorrenza leale e una solida regolamentazione nell'era digitale.

EMFA – Pluralismo dei media – Libertà dei media – Armonizzazione – Basi legali

The Author is Full Professor of Constitutional and Public Law at the University of Florence

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: 1. Introduction. – 2. Two contrasting visions regarding the legal basis of the EMFA. – 2.1. Argument against the chosen legal basis. – 2.2. Arguments in favour of the chosen legal basis. – 3. Two shortcomings regarding the EMFA's approach and the relative counterargument. – 4. Our answer: A different interpretation regarding the "If" of the Regulation. – 5. Conclusions.

1. Introduction

An examination of the evolution of European Union law and policies over the past two decades reveals a growing emphasis on creating a new regulatory framework for media services[1]. At the heart of this initiative is the need to shift from merely protecting media pluralism to actively promoting the freedoms of both recipients of media services and media service providers across all Member States[2].

The principle of media freedom and pluralism is now established in Article 11, paragraph 2, of the Charter of Fundamental Rights of the European Union, reflecting an advancement from previous constitutional and international documents[3]. The drafters of the Charter have decided to emphasise the decisive role of media for European integration in accordance with the constitutional traditions common to Member States and the European Court of Human Rights case law[4]. The aim was to underline the importance of media freedom and independence as a primary guarantee of a democratic system and as a prerequisite for exercising other fundamental rights of citizenship, such as the right to vote, referred to in Article 39(2) of the Charter[5].

The need for new policies in the field of media services at the EU level is evident for several reasons[6]. Firstly, the media and information landscape is in a constant state of evolution and revolution[7]. Secondly, recent crises and conflicts are definitively highlighting the crucial role of the media

1. See Mastroianni 2011; Parcu–Rossi 2021; Holtz–Bacha 2024; Koltay 2024.
2. See the European Parliament resolution of 11 November 2021 on "Strengthening democracy and media freedom and pluralism in the EU: the undue use of actions under civil and criminal law to silence journalists, NGOs and civil society" (2021/2036(INI)) and Council conclusions of 18 May 2021 on "Europe's Media in the Digital Decade: An Action Plan to Support Recovery and Transformation" (2021/C 210/01).
3. Nascimbene–Rossi dal Pozzo 2023; Strozzi 2013.
4. This relevance is underlined primarily by the relevant case-law of the Court of Justice of the European Union, such as *Sky Österreich* (case C-283/11) and *Vivendi* (C-719/18), where the EU judges affirmed that "the preservation of the pluralistic nature of the offer of television programmes, which is intended to guarantee a cultural policy may constitute an overriding reason in the public interest capable of justifying the restriction of the freedom to provide services". For more on this, see Donati 2022.
5. Mastroianni 2022.
6. Malferrari 2023 interestingly stresses three arguments in favour of a new media legislation in Europe: first, digitalisation and the changing media landscape have created a more international media landscape; second, the threat of media manipulation restricts the freedom to provide services and distorts competition in the internal market; third, there is a security threat posed by strategic disinformation as a hybrid threat, especially in times of war.
7. Cole–Etteldorf 2023-b.

sector and its regulation in shaping public opinion, demonstrating its significance in promoting democracy and the rule of law[8]. Thirdly, the recent emergence of Generative Artificial Intelligence has brought to life a powerful tool that can disrupt the information environment and create new global threats[9].

Against this background, approving the "European Media Freedom Act"[10] (EMFA) in 2024 marked a pivotal development in regulating media freedom and completing the regulation of information technologies across Europe[11]. This new Regulation emphasises the EU's commitment to exploring and extending the boundaries of the existing, limited legal framework governing media policy, which primarily focuses on implementing the internal market and enforcing EU competition law[12]. EMFA includes a new European Board for Media Services (EBMS), to replace the European Regulators Group for Audiovisual Media Services (ERGA)[13].

With the EMFA, EU intervention in the media sector has (potentially) evolved towards using dynamically consolidated instruments for market harmonisation and liberalisation[14]. EU institutions have demonstrated a genuine willingness to actively support the media environment in enhancing both the functionality and quality of democracy[15]. However, this evolution faces resistance because it is considered an unauthorised strengthening of EU control over a politically delicate and controversial issue essential for democracy and human rights at the state and local levels[16].

This article discusses a preliminary issue regarding the EU Institutions' willingness to enhance media freedom in Europe: the chosen legal basis for the EMFA. As we know, since the introduction of the proposal for a regulation establishing a common framework for media services in the internal market and amending Directive 2010/13/EU, the Commission expressed the need to use only the legal basis provided by Article 114 TFEU. This latter is set up to adopt measures to approximate the provisions laid down by law, regulation, or administrative action in the Member States, which have as their object the establishment and functioning of the internal market.

Media sector regulation is one of the many areas of the Digital Single Market where this legal basis has been used[17]. The aim of these regulatory initiatives concerning digital technologies is always the same: the EU is taking action through harmonisation instruments to prevent national legislation fragmentation and reclaim European "digital sovereignty"[18], ultimately aimed at better safeguarding fundamental rights and the rule of law. Two significant components underline this policy strategy: firstly, the use of the word "Act"

8. The established "Rule of Law Mechanism" at the EU level devotes a key section to media freedom and pluralism. The first Rule of Law Report covering all 27 Member States, published on 30 September 2020, presented both a synthesis of the rule of law situation in the EU and an assessment of the situation in each Member State, focusing on four main pillars: the judicial system, the anti-corruption framework, media pluralism and other institutional checks and balances. The fifth annual "Rule of Law Report" (2024) highlighted progress and ongoing challenges in the media landscape in all Member States. Despite the signs of progress, the last report expressed persistent concerns about the independent governance and financial stability of public service media, transparency of media ownership, access to public documents and the fair distribution of state advertising. For more information, see European Commission 2024.
9. Bayer 2024-b.
10. Regulation (EU) No. 2024/1083.
11. This regulation completes at least the Digital Service Act, the Digital Markets Act, and the AI Act.
12. Garcia Pires 2017.
13. For other important elements of the new Regulation, see the briefing of the European Parliament.
14. Bayer 2024-a.
15. Holtz–Bacha 2024.
16. Brogi–Parcu 2014.
17. On the importance of Article 114 for the improvement of the Digital Single Market, see Franck–Monti–de Streel 2021; Böttner–Blanke 2023.
18. Fahey–Poli 2022; Müller-Graff 2024.

in the title of these regulations through a process referred to as *act-ification*[19], and, secondly, the establishment of a new governance framework designed to protect specific markets related to the protection of certain fundamental rights[20].

This ambitious objective, which surpasses the previous applications of the legal basis, has been discussed on many occasions so far[21]. Our idea is to stress that the problem of the legal basis manifests a broader and different intensity in the context of the EMFA, which requires a thorough understanding of the role of the EU in the context of media freedom. At the same time, it is essential to explore the implications of this decision for the EU integration process and to assess whether European institutions can fully leverage the powers granted by the new Regulation[22].

2. Two contrasting visions regarding the legal basis of the EMFA

The European Commission has grounded the EMFA proposal solely on Article 114 of the TFEU. This aspect is significant when examining the distribution of powers between the EU and its Member States and whether the Regulation has respected this distribution. Article 114 TFEU allows the adoption of measures relating to the approximation of the laws, regulations, and administrative provisions of the Member States, which have the establishment and functioning of the internal market as their object[23]. Accordingly, to achieve the objectives outlined in Article 26, paragraphs 1 and 2 of the TFEU – namely, to establish or ensure the proper functioning of the internal market with the free movement of goods, persons, services, and capital – the EU is empowered to adopt measures aimed at approximating the laws, regulations, or administrative actions of Member States that pertain to the establishment and functioning of the internal market[24].

Article 114 TFEU serves as a general legal basis that can only be invoked when the Treaties do not offer a more specific legal foundation relevant to a proposed measure. This article does not alter the principle of limited conferral of powers, which dictates that competencies not conferred to the EU remain with the Member States. Furthermore, regarding fundamental rights, Article 6 TEU and Article 51, paragraph 2, of the Charter of Fundamental Rights clearly state that the powers of the EU are neither expanded nor the division of competencies altered.

However, increasing media freedom requires action in areas where the Union has supporting, coordination and complementary competencies. As the EMFA addresses crucial issues of media pluralism[25], a potential legal basis for this could be Article 167 of the TFEU, which pertains to culture and is the sole reference to (audiovisual) media within the TFEU. However, this cultural provision emphasises the cultural sovereignty of EU Member States by avoiding explicit harmonisation measures[26].

Various scholars, policymakers, and now also a Member State[27] have contested the legitimacy of relying solely on Article 114 as the legal founda-

19. Papakonstantinou–De Hert 2022; Cole 2024.
20. Custers 2022.
21. Cole–Etteldorf 2023-a.
22. Monti 2024.
23. As stated by de Witte 2017, Article 114 is the most powerful tool for expanding the EU legislative activity. See also Kosta 2015.
24. Schütze 2014; Weatherill 2016.
25. Grandinetti 2024.
26. The restrictive use of the "cultural clause" is stressed by Cole–Etteldorf 2021.
27. Hungary is currently challenging this decision before the Court of Justice of the European Union. The country argues that differences in national regulations do not warrant the application of Article 114 TFEU, and it also questions the choice of using a regulation instead of a directive. The Action has been brought on 10 July 2024. *Hungary v European Parliament and Council of the European* (case C-486/2024). The Action asks the CJEU, with ten pleas in law, to annul Article 2, point 3, and Article 5; Article 2, point 20, and Article 4; Article 6; Article 7; provisions relating to the European Board for Media Services; Articles 21 to 23; and Article 2, point 19, and Article 25. See on this issues Brogi 2024.

tion for the European Media Freedom Act (EMFA). They raise concerns about whether the European Union is truly capable of achieving this goal in a realm that Member States predominantly govern. In contrast, many individuals have countered this sceptical perspective regarding EU competencies in this area. Let us explore both sides of the argument.

2.1. Argument against the chosen legal basis

The first position emphasises that the EU lacks the power to approve the EMFA, as there is no explicit reference in the Treaties regarding media pluralism[28]. Therefore, it would be better to maintain the power to protect media freedom and pluralism in the Member States jurisdictions because these are issues to be treated at a more national level[29].

Scholars highlight another element. The interpretation of Protocol 29 regarding the system of public broadcasting in the Member States, which is annexed to the Treaty of Amsterdam, underscores that the public service mandate is entrusted to, defined by, and organised by each Member State. The Treaties do not affect the competence of Member States to provide funding for public service broadcasting as long as such funding is allocated to broadcasting organisations to fulfil their public service obligations.

Furthermore, Article 167 TFEU, which explicitly refers to audiovisual media, should be interpreted as confining the EU's competence to the support activities outlined within that article and exclusively in the audiovisual sector[30]. Given these principles and considering media diversity, cultural differences, and national specificities, EU involvement in media regulation could compromise the diversity and independence of national media[31].

Member States are primarily obligated to guarantee freedom of expression for all citizens, a responsibility reinforced by national and supranational courts. Consequently, the EU should focus on regulating only limited and market-related issues of media services rather than legislating on broader concepts of media freedom and freedom of expression (including regulations concerning national security and criminal offences)[32]. Therefore, there is limited potential for expanding EU competencies through the principles of subsidiarity and proportionality to facilitate the regulation of freedom of expression[33]. It is essential to consider the allocation of powers and the limitations on EU action when determining the appropriate legal basis and type of legislative instrument for specific initiatives. Deviating from this approach could jeopardise the principle of conferred competencies, as it may significantly expand internal market competencies in a way that could fundamentally alter the constitutional framework of competence in competition law, as outlined by the Lisbon Treaty[34].

Furthermore, while it is important to recognise that the internal market objective is central to the EMFA, Article 114 TFEU stipulates the necessity of demonstrating actual obstacles to the internal market that the regulation aims to address. Since the EU does not possess the authority to create uniform domestic conditions across all Member States independently, the barriers to trade or pertinent distortions in competition must be evidenced[35].

This position also stresses that the impact assessment accompanying the EMFA proposal deliberately concentrated on sector-specific and country-specific issues rather than broader European concerns that might warrant supranational regulation of freedom of expression. Thus, it would have been more accurate to avoid using the term "fragmentation" and instead focus on the specific challenges faced by individual Member

28. For a complete understanding of this position, see Cole–Etteldorf 2021.
29. Etteldorf 2023.
30. This is the first argument of the Hungarian Action brought in the summer of 2024 (*supra* n. 27).
31. This position is well summarised by Brogi et al. 2023.
32. See also the arguments of the Hungarian Action (*supra* n. 27).
33. See also the arguments of the Hungarian Action (*supra* n. 27).
34. Engel 2023.
35. Etteldorf 2023.

States, particularly Poland and Hungary, along with various media-related regulatory issues[36].

For some scholars, the rules that govern the allocation of powers associated with the EMFA warrant careful examination, particularly concerning the specific legislative instrument chosen for this action[37]. Despite the coherent form of a Regulation, the wording of some parts of the EMFA resembles that of a Directive, leaving the Member States' scope for implementation. However, for some open-ended formulations, such as parts of the chapter on rights and duties, the rules on media market concentration and, especially, the rules on the allocation of economic resources, the harmonising effect of EMFA could lead to challenges in interpretation for Member States[38], resulting in a puzzling situation that would open up controversies on competences.

2.2. Arguments in favour of the chosen legal basis

On the contrary, the second position claims that the EU does have the power to regulate freedom of expression and can use Article 114 TFEU to do so in a more "creative way." In the past decades – as earmarked by the Commission Staff Working Document in 2007 –[39], it became clear that the problem with media pluralism is more complex than one simply arising from the protection against the concentration of ownership in the market[40].

Regulatory frameworks at the national level frequently fail to address the growing concentration of media power due to weak enforcement mechanisms or deliberate inaction driven by political complicity. When systemic failures of democracy are suspected, all social subsystems, including the use of public resources, the economy, and institutional structures, could be in danger[41].

The erosion of media pluralism has numerous harmful effects on EU citizens that extend beyond the borders of individual Member States. Firstly, it hinders the very idea of European integration, including the free movement of media services and persons. Secondly, the goals of the intervention cannot be effectively addressed through the isolated actions of individual states, as the risks at hand are increasingly cross-border and not confined to specific nations[42].

In addition, digital technologies have transformed the media market, especially in financing, distribution, and consumption, so the principles and rules regarding this market, especially pluralism, have acquired a different dimension[43]. Thus, while in the past the problem of pluralism was considered only in the wake of the market players, today we have to consider the issue of protecting consumers' right to choose among many different services[44].

Following this argument, scholars assert that freedom of expression has an EU dimension, which is closely related to the development of democracy in the Union[45]. Therefore, protecting freedom of expression is important for the survival of our supranational institutions. Even the more sceptical scholars regarding Union citizenship acknowledge that safeguarding democracy and freedom of expression is essential to the unwritten social contract among European peoples.

At the same time, giving to the EU institutions only crisis-driven enforcement mechanisms would not protect citizens' freedom of expression adequately. Instead, a methodologically sound,

36. Kozak 2024.
37. Cole 2024.
38. Kerševan 2024.
39. European Commission 2007.
40. Doyle 2002.
41. Tambini 2021.
42. Flear 2017.
43. See Bayer 2024-a: 92 cites an intriguing public lecture by Monroe E. Price at the Central European University on 27 April 2017. During his talk, he discussed the emerging era of "hyper pluralism," in which every conceivable scenario and opinion can be published and is readily accessible.
44. Parcu–Brogi 2021.
45. Brogi et al. 2023.

reliable, permanent and periodic monitoring and evaluation process based on objectivity and equality (monitoring) is recommended to assess potential risks in Member States.

While the regulatory framework governing the media encompasses both cultural and economic aspects, clearly distinguishing between the two is not always feasible. As such, regulating the market dimensions of media services can fundamentally rely on the internal market clause, even though there may be intersections with cultural considerations[46].

In addition, where some find inconsistency, others see the possibility to regulatory cooperation and establishing a framework that is also consistent with the principle of technology neutrality[47].

3. Two shortcomings regarding the EMFA's approach and the relative counterargument

Responding to advocates for new regulatory interventions in media freedom, sceptics highlight two shortcomings inherent to the Commission's policy approach to enacting the EMFA.

The first one regards the category of regulation to which EMFA belongs. The EMFA, together with the DSA, the DMA, the AI Act, and the Data Act, falls into the category of *ex-ante* regulation, mostly directed at specific private operators, stressing the decisiveness of free movement of digital services before competition law applies. While, on the one hand, such regulation has been dictated by the need to realise the markets of the information society, it is also aimed at overcoming the enforcement difficulties of other rules, in particular competition law[48]. The question has arisen regarding whether the market power amassed by online platforms and their ability to create barriers to entry in preferred markets has been effectively and timely addressed through the enforcement of Article 102 TFEU and merger control. Alternatively, it may be argued that the *laissez-faire* approach – and not the excessive fragmentation that has characterised the development and consolidation of the digital market – has contributed to failures within this market and related sectors, such as the media industry, resulting in distortions that necessitate the implementation of sector-specific regulation[49].

In the digital market, where traditional factors of scarcity – such as frequencies and the considerable resources required for disseminating information – are no longer present, the protection of external pluralism by Member States alone does not ensure that all citizens have genuine access to a diverse array of information sources. The information ecosystem offered by the platform economy has additional characteristics inherent in the relationship between competition and pluralism, differentiating it from the old media and creating new scarcities and new "market failures of ideas"[50]. This is the reason why some scholars argue for a "broad base of intervention"[51] that stresses the need for a new understanding of "diversity" (as a way to focus on demand instead of solely supply) and for technical measures that empower the consumer to better choice among alternative options[52].

The second shortcoming addresses the possibility – through the EU's intervention – of treating freedom of expression only as a commodity or service that can be bought and sold in a marketplace. This interpretation, which is far from the doctrine of freedom of expression in many EU countries, can be implied if we stretch the chosen policy option (encouraging undistorted competition, ensuring fair allocation of resources, and avoiding fragmentation), which is used to justify an intervention broader than market regulation. This is also evident in the overlap between premises and consequences in Recital No. 2 of EMFA, where aspects of a cultural nature are prerequisites for the effective provision of services in their eco-

46. Of course, this argument cannot be stretched too much, harming the principle of enumerated powers.
47. Cantero Gamito 2023.
48. Cseres 2024.
49. For a different understanding of this evolution, see Cantero Gamito 2023.
50. Nicita 2024; Manganelli–Nicita 2022.
51. Parcu–Rossi 2021.
52. Manganelli 2023, p. 893 ff.

nomic context[53]. From both fundamental rights and power allocation perspectives, this reasoning may result in framing the concept of freedom of expression within a market context, leaving aside the priority of liberty.

This limitation can indeed be significant. However, the argument broadens the scope of state competencies to such an extent that it introduces considerable rigidity at the EU level. The importance of freedom of expression in today's context far surpasses that of previous eras, as the Digital Single Market increasingly shapes citizens' lives while also posing greater risks than ever before[54].

The unparalleled viral spread of disinformation and hate speech, coupled with the lack of transparency surrounding algorithm-driven news intermediaries, the growing influence of private technology companies in regulating online communication, the polarisation of public discourse, and the diminishing sustainability of traditional news media and journalism, all pose significant challenges to the functioning and legitimacy of democracies across Europe. These issues necessitate a unified response at the EU level[55].

4. Our answer: A different interpretation regarding the "If" of the Regulation

Recognising the EMFA's significance for media freedom in Europe is crucial to understanding and enforcing it, even before delving into its operational details. To encapsulate this perspective, we should emphasise that any discussion regarding the legal foundation of the new Regulation must begin with assessing the "if" involved.

The European Commission embarked on an extensive journey to create the new Regulation that began far beyond its walls. This process involved thorough proposals, discussions, and consultations, reflecting a commitment to gathering diverse perspectives and ideas.

European institutions have long debated the necessity of a unified response to this issue. Numerous European Parliament Resolutions have underscored the increasing threat posed by a lack of media pluralism[56]. The European Citizen Initiative for Media Pluralism of 2015[57] showed the erosion of democracy and the necessity to promote the adoption of European legislation, which could guarantee the independence of the media from economic and political interests[58]. The High-Level Group on Media Freedom and Pluralism created in 2011 recommended an active approach of the EU on media pluralism against the likely restrictions by Member States[59].

The need for specific regulation is also highlighted by the significant emergence of new unregulated and unreliable sources of information, or at other times, cleverly created by foreign authorities or private entities to manipulate electoral processes and destabilise states (as happened even recently with the Romanian case). The possibility of quality information was evident during the Covid-19 pandemic. In this context, it is important to emphasise that the EMFA aligns with the objectives of the EU's "Democracy Action Plan"[60]. This plan aims to promote free and fair elections, enhance democratic participation, support independent media, and combat disinformation through various initiatives.

53. Etteldorf 2023.
54. Parcu–Brogi 2021.
55. Parcu 2020; Malferrari 2023.
56. European Parliament 2013, Resolution on the situation of fundamental rights: standards and practices in Hungary (pursuant to the European Parliament Resolution of 16 February 2012) (2012/2130(INI)) 'the Tavares Report' of 3 July 2013; European Parliament 2015, Resolution on the situation of fundamental rights in the European Union (2013–2014), (2014/2254(INI)); European Parliament 2015, Plenary debate on the 'Situation in Hungary: follow–up to the European Parliament Resolution of 10 June 2015', 2 December 2015.
57. This initiative did not receive enough support as requested by the Regulation (EU) n. 211/2011. For more on the initiative, see 'European Alternatives' website. Unfortunately, the proposal website is not available anymore.
58. Mastroianni 2022.
59. The report concluded that harmonisation of market rules would benefit the EU from multiple points of view. See Vīķe-Freiberga–Däubler-Gmelin–Hammersley–Poiares Pessoa Maduro 2013.
60. European Commission 2020.

In addition, the EMFA proposal coincided with the final stages of the legislative process for the Digital Services Act (DSA) and the Digital Markets Act (DMA). Indeed, the EMFA aims to tackle a disease while acknowledging significant limitations associated with harmonisation in areas beyond the Union's authority. Protecting freedoms involves the most intimate constitutional aspects of each State. Without these, access to the EU is precluded, and, above all, it is impossible to adopt a uniform legislative text among all 27 Member States.

However, the inability of individual Member States to develop an adequate response individually highlights the need to adopt a common European approach. The production and consumption of multimedia content, including news, has become supranational *per se*. For this reason, a common European approach makes it possible to guarantee legal certainty (given the differences between the various Member States' legal systems), fair competition between the various multimedia service providers, and the opportunity for transnational investments to consolidate the sector[61].

With no EU-level policy alternatives available to regulate the digital market, the Commission delved into regulating the internal market. In the absence of a treaty change, the competencies and procedures granted by Article 114 are the only viable path forward, even because they facilitate a high level of parliamentary involvement during the approval phase and establish shared competencies with Member States according to Article 5 TEU[62].

Additionally, it is important to highlight the distinction between Article 114 and the competence outlined in Article 103 regarding "competition". The harmonisation competence related to the internal market allows for greater flexibility in drafting measures, unrestrained by mere competition law objectives[63]. This may include a potentially pre-emptive effect on the entire policy area within the Digital Single Market[64].

This interpretation would also follow the rulings of the Court of Justice of the European Union in famous cases regarding Article 114, such as *Tobacco Advertising*[65], where the CJEU allowed the EU's legislative organs to design measures according to their desired legal base[66]. Furthermore, opting for regulation instead of a directive is justified when considering the need for rapid regulation of the digital market.

From a constitutional law perspective, the shift in the EMFA from media pluralism to media freedom represents a potential constitutional advancement for the EU[67]. The regulation indicates that the Commission prioritised addressing the "distortions" within the internal market and aimed to enhance cross-border competition in the media sector, particularly for audiovisual media services and video exchanges.

Although the Charter of Fundamental Rights of the EU cannot be regarded as a legislative basis for enacting laws at the Union level, the significance of Article 11 should not be overlooked. Its implications extend beyond its apparent scope, as it pertains not only to the Court of Justice – which is required to interpret EU legislation in accordance with the principles of media freedom and pluralism – but also to the political institutions and the European legislator particularly[68]. Even though the harmonising competencies cannot be expanded in a way that adversely affects the interests of Member States, these States must not jeopardise pluralism as a constitutional European value by

61. Authors have stressed the importance of this shift as a new constitutional moment because of this new interpretation of Article 114 TFEU. See Monti 2024.

62. Article 103 TFEU merely requires consultation of the European Parliament, while Article 114 TFEU follows the ordinary legislative procedure with the European Parliament as co-legislator and qualified majority voting in the Council.

63. Fahey 2022.

64. Engel 2023, p. 674.

65. Case C-376/98. *Germany v. Parliament and Council.*

66. Engel–Groussot 2024; Weatherill 2016.

67. Monti 2024.

68. Mastroianni 2022.

justifying national measures that could restrict the free movement of services.

The Union is not only obligated to uphold the general principles that govern the exercise of its competencies – namely, subsidiarity and proportionality – but also, in a more proactive manner, to take into account the sector's specific characteristics[69]. This involves aligning regulatory interventions with the fundamental principles outlined in Articles 2 and 6 TEU (dignity, freedom, democracy, and respect for human rights) as well as the Charter of Fundamental Rights (Article 11). Access to a diverse array of information sources plays a crucial role in enabling informed and conscious engagement in democratic participation rights, including the right to vote, which is recognised within the framework of European citizenship (Article 22 TFEU).

In addition, the inherently transnational nature of the broadcasting of media services cannot be reconciled with a purely national approach to solving the problems of media pluralism and limited EU interventions to purely antitrust rules. This was true in the past with audiovisual media services and is even more critical today after the hybridisation of traditional media and new digital services[70].

Past negative experiences and new worrying situations emerging in other EU Member States called for an urgent common European solution. In this gap, the aforementioned European Citizens' Initiative ("ECI") for Media Pluralism in 2015, which unfortunately did not reach the minimum number of signatories required, aimed to promote the adoption of EU legislation to ensure the independence of the media from political and economic interests. At the same time, the European Parliament has also repeatedly called for EU action on media pluralism[71].

Therefore, the EMFA addresses a critical gap in EU policies regarding harmonising national media ownership regulations and managing conflicts of interest. Given that the Commission has the exclusive authority to propose EU legislation aimed at harmonising national laws to enhance the functioning of the internal market, its failure to submit a proposal would have effectively diminished the likelihood of any EU legislation promoting media pluralism.

If no EU legislation effectively safeguards pluralism for all media services by prohibiting dominant positions in media markets or ensuring media freedom and independence, the EMFA dispels doubts about the lack of a legal basis to regulate media pluralism. Consequently, the arguments we outlined earlier are unconvincing.

Variations and discrepancies in Member States' laws regarding media independence, restrictions on media ownership by individuals in public office, and the disparities within dominant positions in mass media markets present significant threats to the operation of the internal market[72]. Such occasions of market dominance pose a likely threat to freedom of expression. This risky situation has already invoked (and continues to trigger) the EU's authority to legislate under the Treaty articles that focus on harmonising national laws to enhance the functioning of the internal market – with Article 114 TFEU as the stronger basis in supporting this objective.

In this context, the public consultation initiated by the Commission in January 2022, aimed at adopting a new regulation proposal on media freedom based on Article 114 TFEU, is the most effective starting strategy.

Furthermore, the EMFA should be regarded as a vital component of a broader framework that encompasses the regulation of content distribution. Alongside the DSA and DMA, it is essential to consider a network of supplementary secondary legislation and forthcoming proposals, including rules on the transparency and targeting of political advertising, as well as self-regulatory efforts addressing hate speech and disinforma-

69. Smith 2004.

70. Mastroianni 2013.

71. For example, in its resolution of 10 March 2011, the European Parliament called on the Commission to propose a legislative initiative, using its powers in the fields of internal market, competition and audiovisual policy, to define at least minimum standards of media pluralism to be respected by all Member States. See "European Parliament Resolution on Media Law in Hungary", in Eur. Parl. Doc. PVII_TA(2011)0094 (2011), § 6.

72. Valcke–Picard–Zotto et al. 2015.

tion and funding initiatives under the Media and Audiovisual Action Plan[73].

5. Conclusions

It is essential to conclude the legal foundation of the new Regulation. The EU appears to have utilised all available competencies to enhance the protection of media freedom across all Member States. The trend of broadly interpreting Article 114 TFEU is justified and in harmony with safeguarding vital freedoms necessary for ensuring democracy and upholding shared values in Europe. Despite some criticism, there is a substantial consensus among the Commission, the Council, and the Parliament on the need to strengthen EU authority in this field.

Regarding the Member States, two potential scenarios can be envisioned. The first scenario would unfold if they continue to accept the use of Article 114 TFEU as the legal basis for digital regulations. Should this occur, we could witness an erosion of state sovereignty alongside a corresponding strengthening of European technological sovereignty, which may facilitate advancements in the European integration process. However, it remains uncertain whether this outcome will materialise as anticipated. In addition to Hungary, some other countries may seek to challenge and annul future measures to enhance European digital sovereignty. In this sense, the answer of the CJEU will not be the final round but the starting point for the following political and judicial developments.

Against the odds, the EMFA aligns well with the emerging EU legal framework for digital technologies[74], whose cornerstone is the administrative structure for the Digital Single Market. The relationship between traditional and new media necessitates a novel approach to regulating the media market and highlights the need to harmonize this regulation with that of digital services and AI[75].

Concerning specifically the new framework created for the Digital Single Market, a critical question arises: will the responsibilities and powers assigned to this new network of institutions and private entities effectively address the challenges related to freedom of expression across the EU?

This regulation has brought a novel institutional role for the Commission, establishing (in every sector) a network of administrative authorities that actively engages the Member States and private media industries and platforms. A serious question regarding the new framework is whether the responsibilities and powers assigned to this new network of institutions and private entities will effectively address the challenges of freedom of expression across the EU.

The positive answer to this question depends on the ability of all EU institutions to properly use EMFA in three directions: fostering an environment of freedom and opportunity for everyone, deploying technologies aimed at protecting the Digital Single Market from excessive dominance, and ensuring that the preservation of freedom of expression remains a primary goal of all economic activities within it.

References

J. Bayer (2024-a), *Digital Media Regulation within the European Union*, Nomos, 2024

J. Bayer (2024-b), *Legal implications of using generative AI in the media*, in "Information & Communications Technology Law", vol. 33, 2024, n. 3

R. Böttner, H.-J. Blanke (2024), *Article 114 [Harmonisation in the Internal Market]*, in A. Engel, X. Groussot, G.T. Petursson (eds.), "Treaty on the Functioning of the European Union - A Commentary", vol. II, Springer, 2024

E. Brogi (2024), *EMFA Under the Spotlight: Towards a Common Regulatory Framework to Foster Media Pluralism? Introduction*, in "Rivista italiana di informatica e diritto", 2024, n. 2

73. Cole–Etteldorf 2023.

74. Cole 2024; Paolucci 2023.

75. Parcu–Brogi 2021.

E. Brogi, D. Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Union: European Parliament; Policy Department for Citizens' Rights and Constitutional Affairs; Directorate-General for Internal Policies, 2023

E. Brogi, P.L. Parcu (2014), *Evolving regulation for media freedom and pluralism in the European Union*, in "Utilities Policy", vol. 31, 2014

M. Cantero Gamito (2023), *The European Media Freedom Act (EMFA) as Meta-regulation*, in "Computer Law & Security Review", vol. 48, 2023

M.D. Cole (2024), *Acting on Media Freedom: The Proposed European Media Freedom Act (EMFA) of the European Union*, in "University of the Pacific Law Review", 2024, n. 2

M.D. Cole, C. Etteldorf (2023-a), *Future Regulation of Cross-border Audiovisual Content Dissemination: A Critical Analysis of the Current Regulatory Framework for Law Enforcement Under the EU Audiovisual Media Services Directive and the Proposal for a European Media Freedom Act*, Nomos, 2023

M.D. Cole, C. Etteldorf (2023-b), *Research for CULT Committee - European Media Freedom Act. Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, 2023

M.D. Cole, C. Etteldorf (eds.) (2021), *On the Allocation of Competences between the European Union and its Member States in the Media Sector*, Nomos, 2021

K. Cseres (2024), *European competition law, an overlooked element of the EU's rule of law toolbox*, Swedish Institute for European Policy Studies: Sieps 23epa, November 2024

B. Custers (2022), *New digital rights: Imagining additional fundamental rights for the digital era*, in "Computer Law & Security Review", vol. 44, 2022

B. de Witte (2017), *Exclusive member state competences: is there such a thing?*, in S. Garben, I. Govaere (eds.), "The division of competences between the EU and the member states: reflections on the past, the present and the future", Hart, 2017

F. Donati (2022), *Unione europea, libertà e pluralismo dei mezzi di informazione nella proposta di Media Freedom Act*, in "Medialaws", 2022, n. 2

G. Doyle (2002), *Media ownership: The Economics and Politics of Convergence and Concentration in the UK and European Media*, SAGE, 2002

A. Engel (2023), *The Choice of Legal Basis in EU Competition Law: Shifting the Competence in the Digital Era*, in "Europarättslig tidskrift", 2023, n. 4

A. Engel, X. Groussot (2024), *Making the Rule of Law Great Again: The Building of the Digital Rule of Law in the European Union*, in A. Engel, X. Groussot, G.T. Petursson (eds.), "New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights", Springer, 2024

C. Etteldorf (2023), *Why the Words "But" and "However" Determine the EMFA's Legal Basis*, in "Verfassungsblog on matters constitutional", 13 June 2023

European Commission (2024), *2024 Rule of Law Report*, 2024

European Commission (2020), *European Democracy Action Plan: making EU democracies stronger*, 3 December 2020

European Commission (2007), *Media Pluralism in the Member States of the European Union*, Commission Staff Working Document SEC(2007) 32, 16 January 2007

E. Fahey (2022), *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Hart, 2022

E. Fahey, S. Poli (2022), *The strengthening of European technological sovereignty and its legal bases in the Treaties*, in "Eurojus.it", 2022, n. 2

M.L. Flear (2017), *Regulating New Technologies: EU Internal Market Law, Risk, and Socio-Technical Order*, in M. Cremona (ed.), "New technologies and EU law", Oxford University Press, 2017

J. Franck, G. Monti, A. de Streel (2021), *Art. 114 TFEU as a Legal Basis for Strengthened Control of Acquisitions by Digital Gatekeepers*, Legal Opinion commissioned by the (German) Federal Ministry for Economic Affairs and Energy, 20 September 2021

A.J. Garcia Pires (2017), *Media pluralism and competition*, in "European Journal of Law and Economics", vol. 43, 2017, n. 2

O. Grandinetti (2024), *Quale nozione di pluralismo nell'EMFA?*, in "Rivista italiana di informatica e diritto", 2024, n. 2

C. Holtz-Bacha (2024), *Freedom of the media, pluralism, and transparency. European media policy on new paths?*, in "European Journal of Communication", vol. 39, 2024, n. 1

T. Kerševan (2024), *Dalla retorica alla regolamentazione: EMFA e la concentrazione dei media nell'era digitale*, in "Rivista italiana di informatica e diritto", 2024, n. 2

A. Koltay (2024), *Media Freedom and the Law: The Regulation of a Common European Idea*, Taylor & Francis, 2024

V. Kosta (2015), *Fundamental rights in EU internal market legislation*, Hart, 2015

M. Kozak (2024), *The Media Pluralism Principle, The Financing of Public Broadcasters, and EU Law*, in "German Law Journal", vol. 25, 2024, n. 1

L. Malferrari (2023), *Der European Media Freedom Act als intra-vires-Rechtsakt*, in "EuZW–Europäische Zeitschrift für Wirtschaftsrecht", 2023, n. 2

A. Manganelli (2023), *Piattaforme digitali e social network, fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato*, in "Giurisprudenza costituzionale", 2023, n. 2

A. Manganelli, A. Nicita (2022), *Regulating Digital Markets: The European Approach*, Springer, 2022

R. Mastroianni (2022), *Freedom and pluralism of the media: an* European value *waiting to be discovered?*, in Aa. Vv., "Le droit européen, source de droits, source du droit. Etudes en l'honneur de Vassilios Skouris", Mare & Martin, 2022

R. Mastroianni (2013), *Competenze normative dell'Unione europea e disciplina del pluralismo informativo: regolamentazione o concorrenza nel settore audiovisivo?*, in R. Pisillo Mazzeschi, A. Del Vecchio, M. Manetti, P. Pustorino (eds.), "Il diritto al pluralismo dell'informazione in Europa e in Italia", Rai Eri, 2013

R. Mastroianni (2011), *La direttiva sui servizi di media audiovisivi e la sua attuazione nell'ordinamento italiano*, Giappichelli, 2011

M. Monti (2024), *Towards a Federal-Type Regulation of Online Public Discourse by the EU?*, in "European public law", vol. 30, 2024, n. 4

P.-C. Müller-Graff, (2024), *Strategic Sovereignty – Aspects of Its Legal Dimension*, in G. Barrett, P.-C. Müller-Graff, J.-P. Rageade, V. Vadász (eds.), "European Sovereignty: The Legal Dimension", Springer, 2024

B. Nascimbene, F. Rossi dal Pozzo (2023), *L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea, orientamenti giurisprudenziali e recenti interventi normativi*, in "Eurojus.it", 2023, n. 1

A. Nicita (2024), *Il mercato delle verità: come la disinformazione minaccia la democrazia*, il Mulino, 2024

F. Paolucci (2023), *The European Media Freedom Act: (another) new chapter in the digital regulation saga*, in "Diritti Comparati", 6 maggio 2024

V. Papakonstantinou, P. De Hert (2022), *The Regulation of Digital Technologies in the EU: The law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality"*, in "Technology and Regulation Journal", 2022, n. 1

P.L. Parcu (2020), *New digital threats to media pluralism in the information age*, in "Competition and Regulation in Network Industries", vol. 21, 2020, n. 2

P.L. Parcu, E. Brogi (2021), *Introduction*, in P.L. Parcu, E. Brogi (eds.), "Research handbook on EU media law and policy", Edward Elgar Publishing, 2021

P.L. Parcu, M.A. Rossi (2021), *Policy Changes to Strengthen the Protection of Media Freedom and Media Pluralism in the EU*, in P.L. Parcu, E. Brogi (eds.), "Research handbook on EU media law and policy", Edward Elgar Publishing, 2021

R. Schütze (2014), *Limits to the Union's 'Internal Market' Competence(s)*, in L. Azoulai (ed.), "The Question of Competence in the European Union", Oxford University Press, 2014

R.C. Smith (2004), *Rethinking European Union competence in the field of media ownership: The internal market, fundamental rights and European citizenship*, in T. Gibbons (ed.), "Regulating Audiovisual Services", Routledge, 2004

G. Strozzi (2013), *Libertà d'informazione e pluralismo nell'ordinamento dell'Unione europea*, in R. Pisillo Mazzeschi, A. Del Vecchio et al. (eds.), "Il diritto al pluralismo dell'informazione in Europa e in Italia", RaiEri, 2013

D. Tambini (2021), *Media freedom*, Polity Press, 2021

P. Valcke, R.G. Picard, C.D. Zotto et al. (2015), *Indicators for media pluralism*, in P. Valcke, M. Sükösd, R.G. Picard (eds.), "Media pluralism and diversity: Concepts, risks and global trends", Palgrave, 2015

V. Vīķe-Freiberga, H. Däubler-Gmelin, B. Hammersley, L.M. Poiares Pessoa Maduro (2013), *A free and pluralistic media to sustain European democracy*, January 2013

S. Weatherill (2016), *The internal market as a legal concept*, Oxford University Press, 2016

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0213 • articolo sottoposto a peer review • pubblicato in anteprima il 11 mar. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Sofia Verza

What is journalism in the digital age? Key definitions in the European Media Freedom Act

The European Media Freedom Act (Regulation EU 2024/1083) amends the Audiovisual Media Services Directive, updating the list of subjects that can enjoy the safeguards provided in this EU Regulation. For example, it includes press publications in addition to audiovisual broadcasters and – defining who is a Media Service Provider (MSP) – it includes individual journalists and freelancers. The definition of what media are and who is a journalist remains contested though. It seems that EMFA's definition of MSP includes non-profit media and influencers, but excludes other watchdogs (e.g., human rights defenders and civil society organisations), as well as online platforms – thus not granting to these subjects the related rights and duties provided in this Regulation. Among them, the right to protect their sources and not to be subject to intrusive surveillance; and the duty to be independent, and to convey information of public interest following ethical and professional standards. This article will unfold a series of questions related to the nature of the subjects recognized under EMFA, as well as analyse the Act's intertwining with two other key pieces of the European legislative framework that deals with the free flow of plural and independent information: the Digital Services Act (DSA) and the Directive on Strategic Lawsuits Against Public Participation (SLAPPs).

Journalism – Media service provider – Online platforms – Editorial responsibility – EMFA

Cos'è il giornalismo nell'era digitale? Definizioni chiave nello European Media Freedom Act

Lo "European Media Freedom Act" (Regolamento UE 2024/1083) modifica la Direttiva europea sui Servizi di Media Audiovisivi, aggiornando l'elenco dei soggetti che possono godere delle tutele previste da questo Regolamento. Ad esempio, include le testate giornalistiche cartacee e online, oltre alle emittenti radio e TV che erano coperte dalla Direttiva. Definisce inoltre chi è un "fornitore di servizi di media", includendo i giornalisti freelance. La definizione di cosa siano i media e di chi sia un giornalista rimane tuttavia controversa. Sembra che includa i media no-profit e gli influencer, ma escluda altri osservatori (ad esempio i difensori dei diritti umani e le organizzazioni della società civile) e le piattaforme online, non riconoscendo così a questi soggetti i diritti e i doveri previsti dall'EMFA. Tra questi, il diritto di proteggere le proprie fonti e di non essere soggetti a forme di sorveglianza intrusiva; il dovere di essere indipendenti e di riportare informazioni di interesse pubblico seguendo standard etici e professionali. Questo articolo affronta una serie di questioni relative alla natura dei soggetti riconosciuti dall'EMFA e analizza l'intreccio del Regolamento con altri due testi chiave del quadro legislativo europeo che si occupa del libero flusso di informazioni plurali e indipendenti: il Regolamento sui Servizi Digitali (*Digital Services Act* – DSA) e la Direttiva sulle azioni legali strategiche tese a bloccare la partecipazione pubblica (*Strategic Lawsuits Against Public Participation* – SLAPPs).

Giornalismo – Fornitori di servizi di media – Piattaforme online – Responsabilità editoriale – EMFA

The Author is Research Associate, Centre for Media Pluralism and Media Freedom, European University Institute

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: 1. Introduction. – 2. The evolution of the concept of journalism and media. – 3. "Media service providers" under EMFA: journalists, non-profit media, influencers and other watchdogs. – 4. Who carries editorial responsibility? The mild exclusion of online platforms. – 5. Who can enjoy the "media privilege" under Article 18 EMFA? – 6. Final remarks.

1. Introduction

Journalism has been undergoing profound and revolutionary changes in the last two decades: since widespread access to the Internet has been at the disposal of a great amount of people, new ways to access the news as well as new kinds of news producers emerged. From the primordial bloggers and the exchange of information on news forums, the emergence of citizen journalism and then of influencers, to the mounting and quasi-monopolistic role of social media platforms nowadays, the definition of media and journalism became blurred.

The definitory struggle is evident also from a legal perspective: as explained in paragraph 2 of this article, the Council of Europe in particular has been proposing an evolving and increasingly wide definition of media, in line with the digital evolution. Also, the EU regulators have defined what audiovisual media services are in the Audiovisual Media Services Directive (2018) and recently the European Media Freedom Act has proposed a new definition of "media service providers" (MSPs).

Paragraph 3 of this article unfolds Art. 2 EMFA in particular, and the Regulation more at large, to understand how EMFA defines journalism, and if non-profit media, influencers and other watchdogs such as NGOs fall under the MSPs' definition. It is also crucial to explore tangent definitions, such as that of "editorial responsibility", that ultimately lead to the conclusion that online platforms are excluded from being considered MSPs, as they do not hold editorial responsibility over the content present on their services – despite their increasingly quasi-editorial role in granting more or less visibility to the news, or to media outlets' and journalists' accounts through content moderation, or even by removing certain content or accounts. This is analysed in paragraph 4 of this article.

Finally, the EMFA now entrusts platforms to a new task: identifying who are the MSPs' – through the latters' self-declarations of being media made to platforms – and following a privileged procedure during their content moderation practices when dealing with media content and media-related accounts. The so-called "media privilege" provided by Art. 18 EMFA is analysed in paragraph 5 of this article, focusing once again on the crucial point of being defined as news media to enjoy this privilege: this entails being independent, transparent, not AI-generated and, importantly, not to be "rogue media service providers" spreading malicious and propagandistic content.

Understanding with the highest possible amount of legal certainty who the media are and what journalism is nowadays is crucial for a smooth implementation of EMFA. As a matter of fact, MSPs are entrusted with a number of duties and rights – among them the right to protect their sources and not to be subject to intrusive surveillance; and the duty to be independent, and to convey information of public interest following ethical and professional standards. Ultimately, the aim is protecting media from the fierce competition of other actors over the information space, and guaranteeing that citizens continue having the possibility to access diverse and independent news.

2. The evolution of the concept of journalism and media

The journalistic profession is carried on by a variety of actors, working simultaneously and sometimes in a complementary way. Since the concept of

journalism and that of media exist, they have been subject to a continuous negotiation on their meaning and identity, both within but especially outside legal frameworks. First of all, we have journalists – namely persons whose main activity is that of reporting on news and current affairs. Their job consists of different tasks and "faculties", ranging from discovery, examination, interpretation, style and presentation[1]. Journalism studies have engaged in a range of approaches to investigate and define this field: from theoretical and normative studies[2], to empirical ones based on surveys and content analysis – aimed at understanding journalists' self-perceptions and performances[3], to ethnographic work exploring the incoherent borders of the profession[4]. In this regard, an "inherent porousness of journalistic work" has been noted[5]. Journalists can report their stories in a variety of communication means (also called "media"): the press (printed or online), the radio (FM or web), TV (cable, satellite or web), podcasts, newsletters, social media. As we will analyse later in this article, some of these platforms are explicitly defined as media service providers (MSPs) in EMFA and other EU regulations, some others (e.g., social media platforms) don't, with consequences on the range of rights and duties that these actors enjoy. Traditionally, media referred to established institutions such as newspapers, television, and radio, which served as gatekeepers of information. These entities have always played a vital role in shaping public opinion and facilitating democratic discourse, leading to recognise that media are not common goods/services in the market, but they fulfil a democratic role that needs to be recognised in order to shape meaningful media policies. In the rapidly evolving digital age, the traditional concept of media has undergone a profound transformation. Newsrooms and newswork are part of a profession that can best be seen as a self-organizing social system, where different actors meet and intersect and that is dependent on other systems (e.g., publishing and distribution services, or the political system more at large)[6]. The rise of digital platforms, social media, and online content distribution has revolutionised the way information is created, consumed, and shared.

From a policy perspective, the Council of Europe has been proposing a new notion of media from the early 2010s. Recommendation CM/Rec (2011)7 on a new notion of media[7] recognised that a variety of online intermediaries and platforms are "essential" for the media's outreach and individuals' access to media. They have become "essential pathfinders" to information, "gatekeepers", and may have an "active role" (para. 6). The Committee of Ministers recommended that Member States adopt a "broad notion" of media, including

> "all actors involved in the production and dissemination, to potentially large numbers of people, of content (for example, information, analysis, comment, opinion, education, culture, art and entertainment, in text, audio, visual, audiovisual, or other form) and applications which are designed to facilitate interactive mass communication (for example, social networks) or other content-based large-scale interactive experiences (for example, online games), while retaining (in all these cases) editorial control or oversight of the contents" (para. 7).

The Appendix to the Recommendation proposes some elements to identify the media, namely (1) "intent to act as media"; (2) having the "purpose and underlying objectives of media" (3) adhering to professional standards; (4) seeking "outreach and dissemination", where media has traditionally been defined as "mediated public communication

1. Shapiro 2010.
2. Hallin–Mancini 2004.
3. Hellmueller–Mellado 2015. See also the "Journalistic Role Performance" project's methodology and findings.
4. Domingo–Paterson 2011.
5. Carlson–Lewis 2015, p. 7.
6. Deuze–Witschge 2018; Hallin–Mancini 2004.
7. Council of Europe, Recommendation CM/Rec (2011)7 of the Committee of Ministers to member States on a new notion of media, 21 September 2011.

addressed to a large audience and open to all"; (5) meeting public expectation, where individuals expect the media to be "available", and "broadly accessible", even when paid-for services. A broad notion of media is also employed in the 2018 Council of Europe's Recommendation on Media Pluralism and Transparency of Media Ownership[8]. It focuses on online media, defining them as a "wide range of actors involved in the production and dissemination of media content online and any other intermediaries and auxiliary services which, through their control of distribution of media content online or editorial-like judgments about content they link to or carry, have an impact on the media markets and media pluralism"[9]. The specification of these actors' impact on media markets and media pluralism is a key novelty. Moreover, "editorial-like judgments" by intermediaries are also taken under consideration in the 2018 Recommendation on the roles and responsibilities of internet intermediaries, which emphasised that through content moderation and ranking these intermediaries "may thereby exert forms of control which influence users' access to information online in ways comparable to media, or they may perform other functions that resemble those of publishers"[10]. Finally, in 2022, the Council of Europe adopted a Recommendation on principles for media and communication governance, which also elaborated on the "new notion of media"[11]. It emphasises the "heavy dependence" of media on platforms, calling for a "differentiated approach" to media policy when dealing with different actors.

The objective of EMFA is guaranteeing a free and plural access to independent information: it is thus worth noting that from both an academic and a policy perspective – due to the technological development and the rise of digital platforms intermediating media content – the notion of media pluralism is also changing, and has to be reinterpreted[12]. This goes in parallel with a redefinition of the subjects that should be considered as "media".

3. "Media service providers" under EMFA: journalists, non-profit media, influencers and other watchdogs

The crucial provisions of EMFA where the concept of "media" is developed are Art. 2 and Art. 18. Art. 2 lists a series of definitions of relevant subjects and procedures for the whole Act, ranging from the definition of media service provider (MSP) and of editorial responsibility, and encompassing the first definition of media literacy present in a legal text. How these concepts are interpreted influences the whole operationalization of EMFA. Looking closer

8. Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership, 7 March 2018.
9. *Ivi*, at Appendix.
10. Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March, 2018, at Para. 5. See also Valcke–Lambrecht 2019, pp. 282-302.
11. Recommendation CM/Rec (2022)11 of the Committee of Ministers to member States on principles for media and communication governance, 6 April 2022.
12. The European Parliament (EP) also added to the Commission's EMFAProposal a definition of media pluralism, which was then deleted by the Council. The definition was proposed in Art. 2 (13), and described "media pluralism" as "a variety of voices, analyses and opinions in public discourse, including minority positions and opinions, disseminated in an unimpeded way by media service providers which are in the hands of many different owners, each independent from one another, across different media channels and media genres and the recognition of the co-existence of private commercial media service providers and public service media providers"(Amendment n. 93). One of the main criticisms moved to this definition was the lack of a reconceptualisation in light of the technological developments, e.g., to promote "exposure diversity", which should instead be considered as a fundamental aspect of media pluralism together with internal and external pluralism (Brogi–Borges–Carlini et al. 2023; Parcu–Brogi–Verza et al. 2022). The reference to an "unimpeded way of dissemination" of information could also have extended to exposure diversity online, consistently with the additional references to online platforms present in the EP amendments, including the one that adds data from "users of online platforms" among those to be collected for the scope of audience measurement (Amendment n. 94 to Art. 2 (14)), and the one that innovates the definition of "media market concentration". For more reflections on the concept of media pluralism in the EMFA, see Ottavio Grandinetti's article in this special issue.

to the definition of "media service" under Art. 2 (1) EMFA:

> "A 'media service' means a service as defined by Articles 56 and 57 TFEU, where the principal purpose of the service or a dissociable section thereof consists in providing programmes or press publications, under the editorial responsibility of a media service provider, to the general public, by any means, in order to inform, entertain or educate".

Here we encounter the first, relevant novelty of EMFA when compared to the AVMSD: EMFA applies to both print and audiovisual content, including of course the online versions of legacy media as well as digital native media[13]. Under para. 2 of the same Article, a "media service provider" is defined:

> "Media service provider means a natural or legal person whose professional activity is to provide a media service and who has editorial responsibility for the choice of the content of the media service and determines the manner in which it is organised".

Most of the debate regarding the definition of media in EMFA revolves around the absence of two main subjects from the binding articles of the Act, especially in the formulation of Art. 2:

(i) First and foremost, the lack of mention of journalists and journalism[14];
(ii) Secondly, online platforms – in particular social media platforms[15].

It is indeed striking to note that there is no mention of "journalism" or "journalists" in the binding text of EMFA, except for a reference to the protection of "journalistic sources" in Art. 4, shielding media service providers from undue interferences and surveillance[16]. Some mentions of journalism are present in the Recitals, such as Recital 19, stating that "journalists and editors are the main actors in the production and provision of trustworthy media content, in particular by reporting on news or current affairs". The same Recital, together with Recital 9, also includes a reference to freelancers, providing that "media service providers and their editorial staff, in particular journalists, including those operating in non-standard forms of employment, such as freelancers, should be able to rely on a robust protection of journalistic sources and confidential communication". The democratic role of media service providers working on news and current affairs (thus aimed to inform and educate, as distinguished from entertainment) is also recognized in Recital 14, providing the right of recipients to:

> "access quality media services which have been produced by journalists in an independent manner and in line with ethical and journalistic standards and which, therefore, provide trustworthy information. That is particularly relevant for news and current affairs content, which comprises a wide category of content of political, societal or cultural interest at local, national or international level. News and current affairs content has the potential to play a major role in shaping public opinion and has a direct impact on democratic participation and societal well-being. In that context, news and current affairs content should be understood as covering any type of news and current affairs content, regardless of the form it takes".

The reference to "natural persons" in the definition of MSPs (Art. 2 para. 2) should absolutely be interpreted as including journalists; however, the lack of direct mentions of journalism in the binding articles of the Act must be underlined. This has been defined as a "narrow service-based approach", in conflict with the "functional democratic approach" undertaken by European and international human rights law and case law standards (ECtHR, CJEU, CoE)[17], described earlier in this article.

13. "'Programme' means a set of moving images or sounds constituting an individual item, irrespective of its length, within a schedule or a catalogue established by a media service provider" (Art. 2 (4)); "Press publication' means press publication as defined in Article 2, point (4), of Directive (EU) 2019/790" (Art. 2 (5)).
14. Seipp–Fathaigh–van Drunen et al. 2023.
15. Barata 2022.
16. For an in-depth analysis of Art. 4, please read the article by Malferrari 2025.
17. Seipp–Fathaigh–van Drunen et al. 2023.

From this perspective, EMFA would seem to stick to a narrow definition focused on economic activity and professional services, as the AVMSD did, rather than embracing a broader definition recognising the functional role played by journalism in democracy. This service-based approach probably stems from EMFA's (limited) legal base, namely Art. 114 TFUE, aimed at the economic scope of harmonising the internal market[18].

It is not explicitly specified if other media actors, such as civil society organisations (CSOs) and non-profit organisations acting as watchdogs on news, current affairs and public interest issues, could be considered media service providers and consequently enjoy their related rights. As a matter of fact, the SLAPP Directive (2024/1069) aims to grant protection for all "natural and legal persons who engage in public participation on matters of public interest", listing not only journalists, publishers and media organisations, but also "whistleblowers and human rights defenders, as well as civil society organisations, NGOs, trade unions, artists, researchers and academics"[19]. Moreover, as outlined in Recital 9 of the Directive, no precise definition of a journalist is provided in the text, "however, it should be underlined that journalism is carried out by a wide range of actors, including reporters, analysts, columnists and bloggers, as well as others who engage in forms of self-publication in print, on the internet or elsewhere". Basically, this definition seems to exclude only merely private speakers (such as individual social media users disseminating content about private matters) and adopts a "functional approach", based on the democratic function performed by these actors in their actions of reporting on matters of public interest, as opposed to the "service-based" approach. Interestingly, the SLAPP Directive also extends its protection to the platforms disseminating the content of public interest, such as "the internet platform on which they publish their work", "the company that prints a text or a shop that sells the text"[20].

Considering the wide range of duties and rights entrusted to media service providers by EMFA, it could be considered reasonable that the range of subjects for which the Media Freedom Act is applicable is limited compared to the SLAPP Directive. However, the possible exclusion of non-profit media from EMFA's application is to be criticised. As a matter of fact, a key characteristic of the media service providers under Art. 2 (2) EMFA is indeed that the offer of news services is performed as a "professional activity". It is questionable, however, whether this term refers only to situations when such services represent the provider's main source of income or if it should be interpreted as encompassing all media actors respecting journalistic professional standards, thus including also non-profit media. The doubt that the latter may be excluded from enjoying the rights entrusted by EMFA also stems from the reference made by Art. 2 (1), that recalls the definition of "service" as provided by Art. 57 of the Treaty on the European Union which states that such "services" are those "normally provided for remuneration". A strict interpretation may exclude media outlets and journalists working on a voluntary basis or basing their activities on non-profit based business models (e.g., grants or donations), despite their services serving the public interest in providing quality information and respecting professional standards

18. Despite choosing art.114 TFUE as legal basis is mandated by the limitations of the EU's legislative competences, arguably this market-based rationale is not the perfect fit for comprehensively addressing complex phenomena impacting on human rights and societal dynamics (See Parcu–Brogi–Verza et al. 2022, p. 36 ss.). It is fundamental to acknowledge that the EU is essentially an economic regulator. As van Drunen et al. argued «the more the EU enacts rules that affect public communication, the more urgent it becomes to integrate the relevant sets of expertise into EU decision making, strengthen the procedures that anticipate broader impact on the marketplace of ideas, as well as re-think more generally the legitimacy the European Union has for adopting speech-related measures under the legal bases to regulate the internal market and protection of personal data». See van Drunen–Helberger–Schulz–de Vreese 2023.

19. Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation'), Recital 6.

20. *Ivi*, Recital 22.

or adhering to journalistic ethical codes. However, under the case law of the European Court of Justice, it has been established that profit-seeking is not necessary for the qualification as a service[21]. Therefore, there seems to be no impediment for the recognition of non-profit media as MSPs under EMFA. But uncertainty remains as to the exclusion of civil society organizations from the MSP definition instead.

On the other hand, "professional influencers" seem to be included among the MSPs[22]: Recital 9 of EMFA specifies that the definition of media service provider "should exclude user-generated content uploaded to an online platform unless it constitutes a professional activity normally provided for consideration, be it of a financial or other nature". This is confirmed by Paragraph 18 of the "Council conclusions on support for influencers as online content creators" (July 2024)[23]:

> "The European Media Freedom Act (EMFA) lays down common rules for the proper functioning of the internal market for media services, while safeguarding an independent and pluralistic media environment, which can have an impact on the activities of influencers, for instance when influencers are qualified as media service providers".

If influencers can be included among the MSPs – in their activities aimed to inform, entertain or educate – it would mean that they can enjoy the guarantees under, e.g., Art. 4 (*protection from surveillance*) and Art. 18 EMFA (*privileged procedure in content moderation*). However, their adherence to professional and ethical standards, and their editorial independence, could be more problematic to demonstrate than it is for newsrooms and journalists.

The adherence to professional standards should indeed be the basic requirement for the identification of the media service providers that will enjoy the guarantees granted by the EMFA Regulation, in light of the standards elaborated by Recommendation 2022/1634 "on internal safeguards for editorial independence and ownership transparency"[24], accompanying EMFA. As it will be outlined in this article, this is explicitly specified by Art. 18 EMFA as one of the criteria for media service providers to be able to self-declare as media; but the same is not straightforwardly clear under other sections of EMFA, for example in relation with the extent of application of Art. 4 – which prohibits the illegitimate surveillance of media service providers and their sources.

Thus, the principle of legal certainty with regards to the range of subjects who fall under EMFA's implementation seems not to be fulfilled until a more detailed list of criteria for selecting them will be provided by the Commission, the European Board of Media Services (hereinafter, "the Board") and the national regulatory authorities.

4. Who carries editorial responsibility? The mild exclusion of online platforms

The digital revolution has blurred the boundaries between professional journalists and other subjects, enabling anyone with an internet connection to create and disseminate content. Influencers and other platforms' users now play significant roles in the media landscape. Moreover, legacy media outlets – including their online versions – are no longer the gatekeepers of a two-sided market, monetising the attention of the users and sustaining their business mainly with advertising. The media market dramatically suffers from the competition of big tech companies that benefit from lower distribution costs, provide users with content collected from others, and monetise the attention of the users[25].

21. See for example *European Commission v Hungary* (Case C-179/14), 23 February 2016. In paragraph 157. 7 the Court states that "The fact that the national legislation provides that the profits made by the HNRF from that activity must be used exclusively for certain public interest objectives is not sufficient to alter the nature of the activity in question or to deprive it of its economic character".
22. Bayer 2024, p. 119.
23. "Council conclusions on support for influencers as online content creators" (C/2024/3807), 23 July 2024.
24. Commission Recommendation (EU) 2022/1634 of 16 September 2022 on internal safeguards for editorial independence and ownership transparency in the media sector.
25. Brogi–Borges–Carlini et al. 2023.

Art. 2 (2) EMFA provides that a media service provider holds "editorial responsibility for the choice of the content of the media service and determines the manner in which it is organised". The mention of the organisational tasks of MSPs immediately recalls the major role of online platforms, especially social media platforms, in news' dissemination. The same Article, under para. 8, defines "editorial responsibility" as "the exercise of effective control both over the selection of programmes or press publications and over their organisation, for the purposes of the provision of a media service".

This reference might recall the selection and organisation of content operated by the recommender systems of social media platforms, which is also an object of regulation under the Digital Services Act. Recital 11 of EMFA adds that

> "In the digital media market, video sharing platforms or providers of VLOPs could fall under the definition of MSP. In general, such providers play a key role in the organisation of content, including by automated means or by means of algorithms, but do not exercise editorial responsibility over the content to which they provide access. However, in the increasingly convergent media environment, some video-sharing platform providers or providers of very large online platforms have started to exercise editorial control over a section or sections of their services. Therefore, where such providers exercise editorial control over a section or sections of their services, they could be qualified as both a video-sharing platform provider or a provider of a very large online platform and a media service provider".

As noted by Barata, if we were to take this language literally, it would introduce a paradigm change from the current conceptual framework excluding platforms' responsibility for content, under the eCommerce Directive[26]. Content moderation and recommendation practices could be considered a form of exercise of editorial responsibility, and therefore at least certain types of online services would be paired to "traditional" media services[27]. However, this does not seem to be the interpretation that the legislator had in mind. Rather, the definition is aimed at distinguishing media service providers from platform providers but it became sufficiently wide to include platform providers when they have responsibility for the choice of content and in determining the manner in which it is organised[28]. Private exchanges conducted with some EC representatives for the scope of writing this article, clarified that this refers to platforms such as YouTube (which are considered VLOPs under the DSA), that in the "Movies" section assembles catalogues of movies to watch. If this is the case, this mention would designate some of the services identified in the 2018 AVMSD's definition of "video-sharing platform service" (Art. 1 (1.aa)) as possibly holding editorial responsibility.

EMFA also excludes messaging apps from being considered media service providers. Recital 9 specifies that the definition "should also exclude purely private correspondence, such as e-mails, and all services that do not have the provision of programmes or press publications as their principal purpose, meaning where the content is merely incidental to the service and not its principal purpose". Also, private messaging apps such as Whatsapp and Telegram are not considered very large online platforms under the DSA[29] and, consequently, their public channels are not considered as such: for example, channels managed by a news outlet or where single users can enrol and share news content – do not reach the threshold of 45

26. Barata 2022.

27. During the trialogue, the EP also introduced Recital 7a, not present in the final version of EMFA: "The media environment is undergoing major and rapid changes. While the role of the media in a democratic society has not changed, media have additional tools to facilitate interaction and engagement. It is important that media-related policy take those and future developments into account. Therefore, the notion of media used in this Regulation should be interpreted broadly to encompass all actors who are involved in the production and dissemination, to potentially large numbers of people, of content, who have editorial responsibility or who oversee content". Amendment 11.

28. Bayer 2024.

29. European Commission, Supervision of the designated very large online platforms and search engines under DSA.

million users[30]. This means that such services are not required to adhere to the risk assessment and mitigation requirements under Art. 34 and 35 of the DSA for their content moderation activities, nor to apply a privileged procedure for moderating media content under Article 18 EMFA. On the other hand, messaging apps are included in the co-regulatory framework of the Code of Practice on Disinformation (CoP)[31], and from a competition perspective they are taken under consideration under the Digital Markets Act[32]. Two messaging apps – namely Whatsapp and Messenger – are in fact considered core platform services offered by a gatekeeper (Meta)[33].

The role and duties of messaging apps in the latest media policy developments deserve further scrutiny in the near future, considering the increasing role of messaging apps for news dissemination[34]. The DSA and EMFA need to be future proof, and it could be argued that such services should already set up risk assessment and mitigation measures as well as particular strategies to deal with media content, foreseeing that their public channels will reach the status of VLOPs in the forthcoming years.

To conclude these reflections on the role of online platforms in EMFA, one thing clearly differentiates the news media from online platforms and search engines: the imbalance of market and – increasingly – opinion power. This is one of the main issues to be addressed when defining policies to support media freedom and media pluralism, and attempts have been undertaken worldwide to protect news content for example from the perspective of copyright in the digital society, or from the competition perspective[35]. The privileged procedure regarding content moderation of media service providers by VLOPs provided by Art. 18 EMFA can be added to the list.

5. Who can enjoy the "media privilege" under Article 18 EMFA?

As outlined by Caplan and Boyd, the relationship between news media organisations and large online platforms is "isomorphic": the more news media are dependent on platforms for disseminating their content, the more they become more vulnerable to the latter's choices and changes of settings[36]. "When dominant social media companies remove or diminish the visibility of edited content from media service providers, the investment made by these providers effectively goes to waste"[37] and citizens struggle to access quality information from social media platforms.

In order to tackle this issue, Art. 18 EMFA provides a specific procedure for platforms to moderate content produced by media service providers[38]. Following the MSPs self-declaration, in case of content moderation the latter enjoy: (i) expeditious rights to an explanation before the content gets removed; (ii) the right to reply to platforms' action; (iii) the right to lodge a complaint and to engage in

30. See Recitals 14 and 15 of the DSA.

31. See Commitment 25: "In order to help users of private messaging services to identify possible disinformation disseminated through such services, Relevant Signatories that provide messaging applications commit to continue to build and implement features or initiatives that empower users to think critically about information they receive and help them to determine whether it is accurate, without any weakening of encryption and with due regard to the protection of privacy". European Commission, 2022 Strengthened Code of Practice on Disinformation.

32. Vezzoso 2024.

33. Commission Decision of 5 September 2023 designating Meta as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925, C(2023) 6105. Meta can be considered a gatekeeper under Art. 3 (2) DMA, because it fulfils the three cumulative requirements to be designated as a gatekeeper, namely: (i) it has a significant impact on the internal market; (ii) it provides at least one core platform service (CPS) which is an important gateway for business users to reach end users; (iii) it enjoys an entrenched and durable position, in its operations.

34. Reuters Institute 2024.

35. Seipp–Helberger–de Vreese–Ausloos 2024.

36. Caplan–boyd 2018.

37. Bayer 2024, p. 156.

38. Please find a detailed analysis of Art. 18 EMFA in Monti 2024.

a dialogue with the platform; (iv) the possibility to appeal to the Board; (v) platforms are required to report on such practices on a yearly basis[39].

It has been argued that EMFA "aims to kill two birds with a stone"[40]: it both provides regulations on fostering free speech in the EU Member State and integrates the DSA obligations for VLOPs[41]. The ratio is that of recognising the importance of editorial processes for the selection and distribution of information for democratic deliberation, especially when compared to platforms' logics of content recommendation and curation. Moreover, the idea of providing a "privilege" for media content is aimed at balancing the asymmetrical relation of power between media service providers, especially smaller ones, and VLOPs[42].

A similar clause had been discussed as an obligatory "media exemption" or "non-interference principle" in the phase of drafting the DSA, encompassing terms and conditions and notice-and-action procedures. But at that time, no political agreement was reached on this issue; however a debate started which fed into the debate over Art. 18 EMFA[43]. Art. 18 itself faced heavy scrutiny during the trialogue negotiations among European institutions[44]: 20 different amendments were proposed by the EP, making the article lengthy and somehow convoluted.

The first paragraph of Art. 18 EMFA is particularly relevant in conjunction to the question of defining what journalism is and who the media are[45], as this paragraph outlines the conditions under which media service providers can self- declare to VLOPs for their content to enjoy the specific guarantees mentioned above. Among other things, MSPs have to declare that they are editorially independent from political and state actors, to adhere to certain standards for the exercise of editorial responsibility and not to "provide content generated by artificial intelligence systems without subjecting it to human review or editorial control" (Art. 18 (1.e))[46].

EMFA is inherently susceptible to the paradox of media regulation: any legislative effort aimed at affording special protection to the media requires the establishment of a comprehensive definition delineating the parameters of what qualifies as "media", which inherently introduces limitations and the potential for exerting control[47]. As a matter of fact, platforms can reject the MSPs' self-declarations[48]. Counting on platforms' bona fide, it is however worth reminding that these compa-

39. Newly established institution, substituting the European Regulators Group for Audiovisual Media Services (ERGA), as provided by Art. 8 EMFA.

40. Pollicino–Paolucci 2024.

41. Media pluralism and freedom have been added in the final version of the DSA among the fundamental rights that platforms need to respect according to the DSA. This might have a beneficial effect on news media organisations, e.g., preventing platforms from imposing sudden change to their recommendation algorithms that would jeopardise news media's presence online as happened in the past, when posts by news media organisations lost prevalence in favour of user generated content by close profile. See Papaevangelou 2023, p. 471.

42. Bayer 2024, p. 158.

43. Papaevangelou 2023, p. 457. Notably, for the DSA, it was the Committee on Culture and Education of the EP and the Committee on Industry, Research and Energy with Henna Virkkunnen as its opinion Rapporteaur (now EC Commissioner and Executive Vice-President for Tech Sovereignity, Security and Democracy), to propose what became Amendment 511 in the consolidated EP proposal – namely the "principle of non-interference" with editorial content by platforms.

44. van Drunen–Papaevangelou–Buijs–Fathaigh 2023.

45. Papaevangelou 2023, p. 468.

46. With regards to the use of AI in journalism, the Council of Europe has published the "Guidelines on the responsible implementation of artificial intelligence systems in journalism", adopted by the Steering Committee on Media and Information Society (CDMSI) on 30 November 2023, CDMSI (2023)014.

47. Tambini 2023 and Tambini 2021.

48. The VLOPs should publish on a yearly basis the number of rejections and the related grounds (Art. 18 (8.d)), and such decisions can be appealed by also relying on mediation or out-of-court dispute settlement mechanisms.

nies are driven by economic interests and cannot substitute public authorities in deciding the public interest objectives worth pursuing[49].

Three key questions should be raised regarding Art. 18 EMFA and the definition of journalism and media:

(i) What about individual journalists?
(ii) What about other watchdogs?
(iii) What about malicious actors?

(i) The first question – about the status of individual journalists in the system of privileges entrusted by Art. 18 – stems for the duties asked in the self-declaration process, in particular under para. 1.b, where compliance with Art. 6 (1) EMFA is required. The EP and Council added an emphasis on media ownership transparency, by explicitly linking the privilege and the self-declaration process with the transparency requirements listed in Art. 6 (1) (Art. 18 (1.b)).[50] This requires to be transparent regarding direct or indirect owners influencing their operations, or regarding the amount of state advertising received. It is however contestable how this requirement can be fulfilled without prejudices for small newsrooms or single (and eventually, freelance) journalists[51]. In case these subjects would be cut out from enjoying this prioritised procedure in content moderation practices, this would confirm the "narrow service-based" approach to defining media (and their consequent privileges). However, following exchanges with an EC representative on this point, it appears that these subjects could fulfill this requirement simply stating to have nothing to declare with regards to their owner(s) or to state advertising, because they do not have owners outside of themselves, or do not receive state advertising.

(ii) With regards to the second question, the discussion developed a few lines earlier on the stance of human rights defenders and civil society organizations in EMFA remains open. They do not seem to enjoy the privilege granted by Art. 18 EMFA – as the Act undertakes a cautious approach. Arguably, media organisations could still be considered to provide the key infrastructure for journalism to operate in a professional way[52], and this criterion helps over-enlarging the number of subjects that could claim to be entitled to a special treatment when it comes to content moderation activities.

(iii) One of the main arguments of the opponents of a media exemption, already at the time of its proposal for the DSA, is that granting a privileged procedure for editorial content – especially when media are defined in a broad sense – could constitute a loophole for malicious actors to take advantage of such exemption[53]. As a matter of fact, the existence of a media privilege not only raises questions about who are the media, but more specifically about which of them are "good quality", so called "trustworthy" media. The EMFA outlines a series of concepts that help making sense of what is meant by "good journalism" under the Act's rationale: editorial independence and media integrity foremost. One of the declared scopes of EMFA is to safeguard the independence and pluralism of media services (Art. 1); as highlighted by Recital 17 EMFA: "The protection of editorial independence is a precondition for exercising the activity of media service providers and their professional integrity in a safe media environment. Editorial independence is especially important for media service providers which provide news and current affairs content, given its societal role as a public good".

49. Reviglio–Bleyer-Simon–Verza 2024. Again, the question of the legal basis of EMFA under Art. 114 TFUE emerges: in a context characterized by the platformization of the public sphere, Art. 114 TFUE (harmonization of internal market) as the basis for regulating speech-related issues legally recognises the strong ramifications of power of private actors for citizens' fundamental rights, public interests and social values, breaking down the traditional public-private divide (see Vries–Kanevskaia–de Jager 2023, p. 590).

50. Amendment 209.

51. No exceptions for small enterprises are provided in Art. 6 EMFA. Former para. 6 in the Proposal providing in this sense was deleted by the Council and the Parliament. ("The obligations under this Article shall not apply to media service providers that are micro enterprises within the meaning of Article 3 of Directive 2013/34/EU"). See Amendment 142.

52. Nenadic–Brogi 2023.

53. Papaevangelou 2023, pp. 471, 473 and 474. See also *Policy statement on Article 17 of the proposed European Media Freedom Act*, 2023.

The concept of "editorial independence" has been substituted to that of "quality" along the legislative process[54], which is to welcome considering the vagueness and possible arbitrariness in interpreting what "quality content" consists in. However, the concept still appears connected to a series of similar but not completely corresponding concepts, such as those of "editorial integrity" and "media integrity" that will be outlined here following.

The interpretation of the concept of "editorial independence" is particularly relevant in relation to Art. 18 EMFA, being one of the key criteria for MSPs to be able to submit a self-declaration to VLOPs (being independent "from Member States, political parties, third countries and entities controlled or financed by third countries" (Art. 18 (1.e))[55]. The same notion is also crucial for the application of Art. 22 EMFA, providing an "assessment of media market concentrations affecting media pluralism and editorial independence", the so-called "media plurality test" to be performed by national regulatory authorities. However, criticism has been raised regarding the lack of transparency and safeguards of the criteria that should operationalise this notion[56], whose borders are blurred between absence of ownership control, absence of conflicts of interests and the respect for editorial standards based on self-regulatory measures internal to the newsrooms/ respected by individual journalists. Recital 11 of Recommendation 2022/1634, accompanying the EMFA Proposal, states that "Editorial independence shields editors and journalists from conflicts of interest and helps them to resist undue interference and pressure. Therefore, it is a prerequisite for the production and circulation of unbiased information and an essential facet of media freedom". The Recommendation however lists a series of good practices "such as editorial charters or codes or committees of ethics" that could be of inspiration for voluntary self-regulatory measures by news outlets.

The concept of editorial independence is also strictly related to that of media integrity, as Recital 34 EMFA outlines that:

> "media integrity also requires a proactive approach to promoting editorial independence by media undertakings providing news and current affairs content, in particular by means of internal safeguards. Media service providers should adopt proportionate measures to guarantee the freedom of editors to take editorial decisions within the established long-term editorial line of the media service provider. The objective to shield editorial decisions, in particular those taken by editors-in-chief and editors, on specific pieces of content from undue interference contributes to ensuring a level playing field in the internal market for media services and the quality of such services. Those measures should aim to ensure the respect for independence standards throughout the entire editorial process within the media, including with a view to safeguarding the integrity of journalistic content. That objective is also in compliance with the fundamental right to receive and impart information under Article 11 of the Charter. In view of those considerations, media service providers should also ensure the transparency of actual or potential conflicts of interest vis-à-vis the recipients of their media services."

The 2022 Recommendation however does not mention "media integrity", but rather "editorial integrity", where it provides that "media service providers are encouraged to lay down internal rules to protect editorial integrity and independence from undue political and business interests which may affect individual editorial decisions" (Section 1.5). They may include "editorial mission statement, policies to foster a diverse and inclusive composition of newsrooms, or policies on responsible use of sources", "rules aimed to prevent or disclose conflicts of interest", "policies on cor-

54. See the Amendments adopted by the European Parliament on 3 October 2023 on the proposal for a regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act), Amendment 69.

55. Some of these amendments were then rejected by the Council, such as the requirement of independence of the media service providers not only from Member States and third countries, but also from "any Union institution, body, office or agency". See Amendment 210.

56. Seipp-Fathaigh-van Drunen 2023.

rections, including complaint mechanisms", "rules ensuring the separation between commercial and editorial activities" (Section 1.7). These measures seem to fall under the requirement of Art. 18 (1.d) EMFA, requiring that in order to self-declare, MSPs have to "declare that they are subject to regulatory requirements for the exercise of editorial responsibility in one or more Member States and to oversight by a competent national regulatory authority or body or that they adhere to a co-regulatory or self-regulatory mechanism governing editorial standards that is widely recognised by and accepted in the relevant media sector in one or more Member States". All the measures suggested in the 2022 Recommendation however have a self-regulatory nature and are difficult to envisage as effectively in place in the short-time, especially in countries, contexts and media systems where such practices are not common nor part of the journalistic culture and professional routines[57].

It is thus rather expectable that – for some time after the entrance into force of EMFA in August 2025 – most of the efforts related to the self-declarations under Art. 18 EMFA would focus on preventing "rogue media service providers" (the most insidious category of non-independent MSPs) from accessing the "media privilege". This urge is increased by the understanding that in various recent electoral appointments in the EU, including the 2024 European elections, shortcomings in the rule of law as well as in the free flow of independent information undermined the democratic functioning.

In this regard, Recital 49 of EMFA provides that a list of criteria should be drafted by the Board "to further support national regulatory authorities or bodies in their role of protecting the internal market for media services from rogue media service providers". The list would concern:

> "media service providers established or originating from outside of the Union. Such a list would help the national regulatory authorities or bodies concerned in situations where a relevant media service provider seeks jurisdiction in a Member State or where a media service provider already under the jurisdiction of a Member State appears to pose a serious and grave risk to public security. Elements to be covered in such a list could concern, inter alia, ownership, management, financing structures, editorial independence from third countries or adherence to co-regulatory or self-regulatory mechanisms governing editorial standards in one or more Member States".

This formulation recalls the binding one of Art. 18 (1.d) EMFA, but only referring to foreign MSPs[58]. According to Recital 53 EMFA, it should be the Commission to instead provide guidelines regarding the implementation of the self-declaration functionality "minimising the risks of abuse" by rogue MSPs established and originating from within the EU. Standards and goals need to be developed, and the journalistic community will need to be actively involved, and to take a stance.

In order to facilitate the recognition of MSPs that are independent and adhere to professional standards, various attempts of certifications and labelling are being experimented. As a matter of fact, the quality of news services could be considered as an essential characteristic for the economic product of media services, to provide a basis for mutual recognition in the internal market. In this regard, parallels with the certifications and labels for products' standards, e.g., in the food safety chain, have been suggested.[59] In particular, the Journalism Trust Initiative (JTI) has decided to

57. Moreover, increasingly news media also combine news and current affairs with entertainment content, combined with click-baiting tactics, easily sharing unverified, oversimplified and disinformation narratives. This damages the reputation of journalism and makes it harder to argue in favor of a media privilege towards these subjects. However, when sustainable, independent, and trusted, media are best positioned to debunk disinformation narratives by providing accurate and complete information to citizens. See Nenadic–Brogi 2023.

58. Moreover, MSPs originating from outside the Union can also be subject to "coordinated measures" by the Board and national regulatory authorities, under Art. 17 EMFA.

59. Bayer 2024, p. 115; similar proposals have been formulated regarding algorithmic recommender systems and parallels with the use of nutrition labels. Detraction points consist in the dynamic nature of algorithmic systems, as well as the lack of a consolidated science and enforcing body in this field. The same could be said with regard to labelling media outlets and media content. See also New research from NYU shows NewsGuard helps those

translate existing ethical and professional standards of journalism into an industry standard of journalistic processes[60]: group of international experts have come up with a general standard that is now listed as an ISO standard, one which allows media outlets to self-assess and to be certified. It translates into a machine-readable code that allows platforms' algorithms to recognise the content and to increase its visibility. Recital 53 suggests that, where relevant, VLOPs should rely on this standard[61].

All this said, the "media privilege" is in practice not more than a fair procedure: to provide a reasoned notification prior to take-down and the right of the interested party to reply within 24 hours. Procedural fairness is a prerequisite for safeguarding freedom of expression[62], but the right to prior informing is hardly more than a symbolic gesture to media service providers[63]. Some civil society organizations proposed to expand the privilege to actually promote the visibility of independent MSPs' content[64]. The actual impact on the quality of the information environment remains to be seen for the near future. For example, it appears that the cases when Art. 18 could be applied are limited: it is specified that this would be the case only outside the systemic risks scenarios under Art. 28, 34 and 35 of the DSA, for example in relation to content moderation practices tackling disinformation, or illegal content such as hate speech, cyber violence, or measures aimed at the online protection of minors (Art. 18 (4)). It seems legitimate to wonder then: when will Art. 18 be actionable?[65]

As it stands now, and without the possibility of evaluating its practical implementation yet, Art. 18 appears to be a convoluted procedure to guarantee procedural safeguards. However, indeed, Art. 18 EMFA opened the way for developing a "new social contract", defining the status of the media in the digital society[66]. It stands as the only legislative attempt at the EU level to explicitly promote the principle that media and journalism, as key democratic institutions, should not be censored by VLOPs and VLOSEs. It therefore becomes fundamental to preserve this normative principle as well as to provide sufficient clarity and flexibility for the Article to make its applicability effective and long-lasting[67].

6. Final remarks

Who are the media, who decides upon this and why should they be granted special privileges are problematic questions that require normative choices to be answered.

most exposed to misinformation – NewsGuard (newsguardtech.com) and What 'Nutrition Facts' Labels Leave Out | TIME

60. The Journalism Trust Initiative. Another initiative is IWA 44, a unique identifier for media outlets (similar to DOI).

61. Recital 53 EMFA: "Where relevant, providers of very large online platforms should rely on information regarding adherence to those requirements, such as the machine-readable standard of the Journalism Trust Initiative, developed under the aegis of the European Committee for Standardisation, or other relevant codes of conduct. Recognised civil society organisations, fact-checking organisations and other relevant professional organisations recognising the integrity of media sources on the basis of standards agreed with the media industry should also have the possibility to flag to the providers of very large online platforms any potential issue regarding compliance by media service providers with the relevant requirements for the self-declaration.

62. Bayer 2022.

63. Bayer 2024, p. 161.

64. Reporters Without Borders 2023.

65. With regards to content moderation practices towards media service providers, EMFA results to be a lex specialis in relation to the DSA. Connections with the DSA can be found in relation with: (i) the definition of editorial responsibility under Art. 2 (8) of EMFA – mentioning the control both over the choice of content and its organisation as criteria for identifying such responsibility; (ii) the mentioning of VLOPs and video-sharing platforms as possibly having editorial responsibility under Recital 11; (iii) The special status of media service providers vis-a-vis VLOPs' content moderation practices under Art. 18 EMFA. See Pollicino–Paolucci 2024, p. 8.

66. Tambini 2023.

67. Nenadic–Brogi 2023.

Ultimately, the scope of media policies is guaranteeing the thriving of free and diverse media service providers, consequently enabling citizens to access independent information meeting their information needs, enabling them to evaluate the world they live in, and undertaking informed choices in their daily life and in the context of their civic participation. This is why defining who are the media to be protected – and from which to pretend a certain degree of transparency and the respect of editorial independence and professional standard – is crucial.

It appears that EMFA puts in place, by means of inclusion or exclusion in the category of "media service provider", different categories of media: independent MSPs, not independent MSPs, rogue MSPs (the most insidious category of non-independent MSPs). This is done through the use of tangent categories, such as the definition of "service" under the Treaty on the Functioning of the EU and the concepts of "editorial responsibility" and "editorial independence". As a consequence, non-profit media and influencers seem to fall under the definition of MSPs, while other watchdogs like civil society organizations are excluded. Social media platforms are also excluded, not holding editorial responsibility despite the increasingly editorial role in content moderation practices. However, they are required to identify the MSPs operating on their services, and to grant them with a special procedure when their content is subject to content moderation. Despite such a privileged procedure appears to be weak in protecting and enhancing the prominence of independent journalism, it stimulates discussions regarding a new definition of what constitutes trustworthy media or journalism[68], looking at the list of criteria provided by Art. 18 EMFA for MSPs' self-declarations to platforms: being independent from political entities, being transparent about their funding, adhering to professional standards, not providing AI-generated content without human oversight.

EMFA is a principle-based Regulation, thus its implementation – mostly starting in August 2025 – remains to be observed. However, as a Regulation, it is directly and literally applicable not only to Member States but to other legal subjects as well, including legal entities and natural persons; namely, it will be directly applicable by and on media companies, journalists and online platforms too, among others. That is why speculating on the interpretation of concepts put forward by EMFA, and in particular on the very subjects of this Regulation, is crucial and must be done before its entrance into force, so that the field is clear, and all stakeholders could make the most out of this regulatory effort.

References

J. Barata (2022), *Protecting Media Content on Social Media Platforms. The European Media Freedom Act's Biased Approach*, in "Verfassungsblog: On Matters Constitutional", 25 November 2022

J. Bayer (2024), *Digital Media Regulation within the European Union. A Framework for a New Media Order*, Nomos, 2024

J. Bayer (2022), *Procedural rights as safeguard for human rights in platform regulation*, in "Policy & Internet", 2022

E. Brogi, D. Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, Study required by the LIBE Committee, July 2023

R. Caplan, D. Boyd (2018), *Isomorphism through algorithms: Institutional dependencies in the case of Facebook*, in "Big Data & Society", vol. 5, 2018, n. 1

M. Carlson, S.C. Lewis (eds.) (2015), *Boundaries of Journalism. Professionalism, Practices and Participation*, Routledge, 2015

68. Bayer 2024, p. 159.

M. Deuze, T. Witschge (2018), *Beyond journalism: Theorizing the transformation of journalism*, in "Journalism", vol. 19, 2018, n. 2

D. Domingo, C. Paterson (eds.) (2011), *Making Online News*, Peter Lang, 2011

O. Grandinetti (2024), *Quale nozione di pluralismo nell'EMFA?*, in "Rivista italiana di informatica e diritto", 2024, n. 2

D.C. Hallin, P. Mancini (2004), *Comparing Media Systems: Three Models of Media and Politics*, Cambridge University Press, 2004

L. Hellmueller, C. Mellado (2015), *Professional roles and news construction: A media sociology conceptualization of journalists' role conception and performance*, in "Communication & Society", vol. 28, 2015, n. 3

L. Malferrari (2025), *Rights of Media Service Providers*, in "Rivista italiana di informatica e diritto", 2025, n. 1, forthcoming

M. Monti (2024), *The missing piece in the DSA puzzle?Article 18 of the EMFA and the media privilege*, in "Rivista italiana di informatica e diritto", 2024, n. 2

I. Nenadić, E. Brogi (2023), *Why news media need article 17 of the European Media Freedom Act*, 16 November 2023

C. Papaevangelou (2023), *'The non-interference principle': Debating online platforms' treatment of editorial content in the European Union's Digital Services Act*, in "European Journal of Communication", vol. 38, n. 5

P. Parcu, E. Brogi, S. Verza et al. (2022), *Study on media plurality and diversity online – Final report*, European Commission: Directorate-General for Communications Networks, Content and Technology, Publications Office of the European Union, 2022

O. Pollicino, F. Paolucci (2024), *Unveiling the Digital side of Journalism: Exploring the European Media Freedom Act's opportunities and challenges*, in "La Revue des Juristes de Sciences Po", 2024, n. 1

Reporters Without Borders (2023), *Increase ambition and consistency of the European Media Freedom Act (EMFA)*, May 2023

Reuters Institute (2024), *Digital News Report 2024*

U. Reviglio, K. Bleyer-Simon, S. Verza (2024), *Governing Social Media's Opinion Power: the Interplay of EU Regulations*, in "MediaLaws", special issue "L'impatto di Internet e dell'intelligenza artificiale sul diritto all'informazione e alla comunicazione", 2024, n. 1

T. Seipp, R.Ó. Fathaigh, M. van Drunen (2023), *Defining the 'media' in Europe: pitfalls of the proposed European Media Freedom Act*, in "Journal of Media Law", vol. 15, 2023, n. 1

T.J. Seipp, N. Helberger, C. de Vreese, J. Ausloos (2024), *Between the cracks: Blind spots in regulating media concentration and platform dependence in the EU*, in "Internet Policy Review", vol. 13, 2024, n. 4

I. Shapiro (2010), *Evaluating journalism: Towards an assessment framework for the practice of journalism*, in "Journalism Practice", vol. 4, 2010, n. 2

D. Tambini (2023), *The EU is taking practical measures to protect media freedom. Now we need theory*, CMPF Discussion Series, May 2023

D. Tambini (2021), *What is journalism? The paradox of media privilege*, in "European Human Rights Law Review", 2021, n. 5

P. Valcke, I. Lambrecht (2019), *The evolving scope of application of the AVMS Directive*, in P.L. Parcu, E. Brogi (eds.), "Research Handbook on EU Media Law and Policy", Edward Elgar Publishing, 2019

M. van Drunen, N. Helberger, W. Schulz, C. de Vreese (2023), *The EU is going too far with political advertising!*, in "DSA Observatory", 16 March 2023

M.Z. van Drunen, C. Papaevangelou, D. Buijs, R.Ó. Fathaigh (2023), *What can a media privilege look like? Unpacking three versions in the EMFA*, in "Journal of Media Law", vol. 15,2023, n. 2

S. Vezzoso (2024), *'Super-apps' and the Digital Markets Act*, in "Journal of Antitrust Enforcement", vol. 12, 2024, n. 2

S. Vries, O. Kanevskaia, R. de Jager (2023), *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, in "European Papers", vol. 8, 2023, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0214 • articolo sottoposto a peer review • pubblicato in anteprima il 27 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Luigi Malferrari

New and reinforced rights for media service providers under Article 4 European Media Freedom Act

The free exercise of economic activity in the media sector is important both for the EU internal market and for the free media as a public watchdog. Article 4 of the European Media Freedom Act (EMFA) imposes on Member States the obligation to respect the media service providers' effective editorial freedom and independence. Article 4 EMFA protects in particular journalistic sources and confidential communications against both traditional forms of interference and spyware. The obligation of prior judicial authorization and a stringent justification and proportionality test are amongst the guarantees laid down in Article 4 EMFA. It "europeanizes" and "proceduralizes" the issues. It, furthermore, introduces a new guarantee consisting in an independent authority or body to provide assistance with regard to the exercise of the right to effective judicial remedy. Economic efficiency and the protection of the EU values are reconciled in Article 4 EMFA. Thus, the EMFA also strengthens the bond that holds individuals and society together in Europe.

Media service providers – Editorial freedom and independence – Internal market – Fundamental rights – EU values

Diritti nuovi e rafforzati per i fornitori di servizi media ai sensi dell'articolo 4 dello European Media Freedom Act

Il libero esercizio dell'attività economica nel settore dei media è importante sia per il mercato interno dell'Ue sia per la libertà dei media come "cane da guardia" pubblico. L'articolo 4 della legge europea sulla libertà dei media (EMFA) impone agli Stati membri l'obbligo di rispettare l'effettiva libertà editoriale e indipendenza dei fornitori di servizi mediatici. L'articolo 4 EMFA protegge, in particolare, le fonti giornalistiche e le comunicazioni riservate sia dalle forme tradizionali di ingerenza sia dallo spyware. L'obbligo di previa autorizzazione giudiziaria e un rigoroso test di giustificazione e proporzionalità rientrano tra le garanzie di cui all'articolo 4 dell'EMFA. Esso "europeizza" e "giuridifica" le questioni; introduce inoltre una nuova garanzia costituita da un'autorità o da un organismo indipendente per fornire assistenza nell'esercizio del diritto a un ricorso giurisdizionale effettivo. L'efficienza economica e la protezione dei valori dell'Ue trovano una riconciliazione nell'articolo 4. Pertanto, l'EMFA rafforza anche il vincolo che mantiene insieme gli individui e la società in Europa.

Fornitori di servizi mediatici – Libertà editoriale e indipendenza – Mercato interno – Diritti fondamentali – Valori dell'Ue

The Author is member of the Legal Service of the European Commission and lecturer at the Europa-Institute of the University of Saarland and at SciencesPo of the R. Schuman University of Strasbourg. The opinions expressed are purely personal

The Author thanks Maximilian Gerhold, Thomas Giegerich, Jan Kermer, Serena La Pergola, Audrius Perkauskas, Sofia Verza and Dirk Voorhoof for precious input. Any error of fact or law is attributable to the author only

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: 1. Introduction. – 2. The content of Article 4 EMFA: how many rights, and for whom? – 2.1. Article 4(1) EMFA: general clause with added normative value. – 2.2. Article 4(2) EMFA: the protection of editorial freedom and independence of media service providers. – 2.3. Article 4(3) and (8) EMFA: the protection of journalistic sources and confidential communications and the right to effective judicial protection. – 2.4. The national security dispute. – 2.5. Regulating spyware as the "major novum" under Art. 4 EMFA. – 3. The issue of legal basis: media-specificities and misunderstandings? – 4. The future prospects of enforcement of Article 4 EMFA. – 5. Conclusion.

1. Introduction

The media sector has dramatically changed in the last few decades. This change is still ongoing. Digitalization (including platformization) has been a major factor in the modernization and internationalization of the media, bringing with it new opportunities but also making the media sector increasingly complex and problematic[1]. This change has disrupted the traditional business model and the financial viability of media outlets as well as journalists' employment prospect[2]. The 2008 financial crisis has magnified these negative aspects, bringing further distress to the viability of the media and to the professional stability of journalists[3]. In addition, media freedom has been under strain, in particular due to the fact that governmental intervention and disinformation, including from third countries, have put into question the media public space in the EU[4]. Moreover, sensationalist and provocative content is often used to maximize engagement rates and advertising revenues and in turn it is amplified by the algorithms of Internet platforms[5]. The market power of Internet platforms is reinforced by the fact that only they have integrated ecosystems and the huge amount of data necessary for the optimal use of algorithms.

Against this backdrop, the European Media Freedom Act (EMFA) was enacted in the spring of 2024 after the Commission's proposal in September 2022[6]. The EMFA is in several regards a remarkable piece of EU legislation[7]. To begin with, the EMFA is the first piece of EU legislation that introduces a comprehensive regime for media services. It, thus, occupies a terrain that was traditionally understood as belonging to national legislation – understanding that was there despite the existence of the fundamental freedoms and

1. See the Explanatory Memorandum accompanying the Commission Proposal, COM(2022) 457, pp. 8-9; Council conclusions on safeguarding a free and pluralistic media system, § 21 (OJ of 7 December 2020, C 422/8); Reuters 2024.
2. Bayer 2024, p. 89.
3. *Ivi*, p. 91.
4. See also Raab 2022.
5. Council conclusions on safeguarding a free and pluralistic media system (2020), § 32.
6. Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (COM/2022/457).
7. See also Cornils 2024.

of the Audio-Visual Media Services Directive[8]. Secondly, the EMFA is remarkable because it concerns one of the most sensitive aspects of our society: the media is a very special economic sector which is politically and culturally loaded, and at the same time, it constitutes a crucial aspect of our democracies due, inter alia, to its public watchdog function[9]. Not surprisingly, the EMFA has been denounced by some political, academic and economic constituencies, while it has been praised by journalist associations, liberal governments, NGOs and progressive academicians.

Within the EMFA, a special and central place is occupied by Article 4, which is titled "Rights of media service providers". Indeed, the protection of the media service providers' rights plays a crucial role in the EMFA ecosystem because this act aims at developing the internal media market and, at the same time, defending the pluralism and independence of the media (cf. Article 1 and recital 2 EMFA)[10]. According to the European Parliament's rapporteur for the EMFA, one of the most important achievements of the Act is the clear definition of safeguards for media providers, including public service broadcasters under Article 5 EMFA, against undue influence by Member States[11]. It is, thus, not surprising that Article 4 EMFA was probably the most debated provision during the legislative process, as the different versions by the Council and the European Parliament (EP) and the Commission's proposal testify[12].

In the present essay, the essential features of Article 4 EMFA are presented. Thereafter, I tackle the question of the extent to which Article 4 EMFA introduces a new normative approach or simply restates existing ones. In addition, the dispute regarding national security is deconstructed and the meaning of paragraph 9 of Article 4 EMFA is explained ("The Member States' responsibilities as laid down in the TEU and the TFEU are respected"). Furthermore, the issue of the EMFA's legal basis is examined. Finally, the future prospects of enforcement of Article 4 EMFA are discussed.

2. The content of Article 4 EMFA: how many rights, and for whom?

2.1. Article 4(1) EMFA: general clause with added normative value

Article 4 EMFA starts in paragraph 1 with a general proposition: "Media service providers shall have the right to exercise their economic activities in the internal market without restrictions other than those allowed pursuant to Union law". The provision lays down an individual's right, as the wording and the title of the provision indicate and as follows from the objective of the provision explained in particular in recitals 17 and 18 EMFA.

Article 4(1) EMFA might *prima facie* appear tautological: isn't the right to exercise the media service providers' economic activity in the internal market without restrictions already laid down in the freedom of establishment (Article 49 TFEU) and the freedom to provide services (Article 56 TFEU)? The answer is in the positive, however with an important caveat: the fundamental freedoms under the Treaty apply only where there is a cross-border element. By contrast, Article 4(1) EMFA bestows upon media service providers the right to exercise their economic activities in the internal market *tout court*, regardless of the presence of a cross-border element. Therefore, Article 4(1) EMFA is not purely declaratory in nature[13]. In secondary law, the EU legislator may set out rules

8. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).
9. See to this effect Bayer 2024, p. 96.
10. As regards the notion of pluralism see Jakubowicz 2015; Valcke–Picard–Dal Zotto 2015.
11. Verheyen 2024.
12. See in particular European Parliament IMCO's Opinion of 3 March 2023, 2022/0277(COD); European Parliament CULT Committee's Opinion of 31 March 2023, 2022/0277(COD); Council's text constituting the Mandate for negotiations with the European Parliament of 21 June 2023, 10954/23; European Parliament's draft position in view of the negotiation with Council adopted on 7 September 2023. See also Cornils 2024, under II, 1.
13. But see Ferreau 2024, p. 40.

that apply also in an intra-national context[14]. *En passant*, it should be noted that, since Article 4 EMFA particularizes the freedom of establishment and the freedom to provide services and given the absence of any indication to the contrary, the term "restriction" used in this provision should be given the same meaning as under Articles 49 and 56 TFEU: it is any measure emanating from the State or quasi-State authority or entities entrusted by the States where that measure is liable to prohibit, hinder or make less attractive the exercise of the media service providers' activity. That definition includes the measure that indirectly emanates from the State in the sense that the State uses a private party as *longa manus* of its action[15]. It is plausible that the term "restriction" in Article 4 EMFA also includes the measures enacted by associations capable of regulating the economic sector in a collective manner, which follows under certain conditions into the ambit of application of the fundamental freedoms[16]. That interpretation would follow from the need for harmony between Article 4 EMFA and the fundamental freedoms. It is an open question whether the ambit of application of Article 4 EMFA can include the deployment of spyware used by any private entity against journalists. Whereas that option has been advocated on the basis of valid policy considerations[17], it remains difficult to reach that result through legal exegesis.

Article 4(1) EMFA further provides that the media service providers' activities in the internal market is to be exercised "without restrictions other than those allowed pursuant to Union law". Is this clause stating only the obvious? If a national restriction is mandated by EU law (e.g. one of the obligations that Member States must apply regarding media market concentrations in compliance with Art. 22 EMFA; or a national measure imposed in compliance with the EU Unfair Commercial Practices Directive), it will qualify as being "allowed pursuant to Union law" in the meaning of Article 4(1) EMFA. By the same token, if a restriction is imposed by national authorities without being mandated by EU law, it needs to comply with the existing EU rules such as the freedom of establishment and the freedom to provide services. As a result, the restrictions to the economic activity of media service providers can be accepted only if they are either mandated or permitted under EU law. That is not superfluous because it clarifies the boundaries for Member States' intervention. It is also in line with the minimum harmonization clause laid down in Article 1(3) EMFA, because this clause provides for the possibility that Member States go further than the EMFA provisions however under the condition of higher protection for media pluralism or editorial independence. This is clarified in recital 8 EMFA, whereby "Member States should have the possibility to adopt more detailed or stricter rules in specific fields, provided that those rules ensure a higher level of protection for media pluralism or editorial independence in accordance with this Regulation and comply with Union law and that Member States do not restrict the free movement of media services from other Member States which comply with the rules laid down in those fields". Moreover, the last part of Article 4(1) EMFA has one additional function, namely to occupy the legislative ground in the field of media law; that may play a role in the assessment of the question of whether the Union has exercised in this field its legislative competence pursuant to Article 3(2) TFEU, which in turn determines the exclusive competence of the Union for the conclusion of an international agreement.

2.2. Article 4(2) EMFA: the protection of editorial freedom and independence of media service providers

Paragraphs 2 and 3 of Article 4 EMFA set out more specific rules than paragraph 1. They follow the 2-step scheme that is typical of the fundamental freedoms: first, a prohibition of principle and then, a derogation. The derogation is subject to numerous detailed conditions, which constitute the *plat de résistance* of the provision.

Paragraph 2 of Article 4 EMFA protects the editorial freedom and independence of media service providers. It is formulated as an obligation for the

14. Judgment of 30 January 2018, *Visser*, C-360/15, EU:C:2018:44, §§ 98-110.
15. See expressly recital 25 EMFA (*in fine*) as regards spyware.
16. Cf. judgment of 12 December 1974, *Walrave and Koch*, 36/74, EU:C:1974:140, § 17.
17. Kermer 2024-a.

Member States ("Member States shall respect…"). That circumstance however does not lead to the conclusion that it is not an individual's right for media service providers. Upon proper construction, it is in fact an individual's right. Indeed, to begin with, the title of Article 4 EMFA is "Rights of media service providers"[18]: the plural form ("Rights") indicates that there is more than one right laid down in the Article, i.e., more than the right expressly laid down in paragraph 1 of Article 4 EMFA. Then, the purpose of the provision is the protection of the editorial independence (see recital 17 EMFA). More precisely, the objective is "to put in place effective safeguards enabling the exercise of editorial freedom across the Union so that media service providers can independently produce and distribute their content across borders and recipients of media services can receive such content" (recital 18 EMFA). Furthermore, in EU law, individual rights can flow from obligations imposed on Member States, as is the case, for example, for the rights that are bestowed upon individuals by the free movement rules of the Treaty, which are addressed to the Member States[19]. In addition, a systematic element also indicates that Article 4 EMFA grants rights to individuals: since Article 4 EMFA specifies the content of the freedom of establishment and the freedom to provide services (which grant rights to individuals), the existence of rights of individuals should be recognized for Article 4 EMFA, too. Finally, still from a systemic viewpoint, Article 3 EMFA (the "sister" provision to Article 4 EMFA) must be taken into account. Under this provision, "Member States shall respect the right of recipients of media services to have access to a plurality of editorially independent media content and ensure that framework conditions are in place in line with this Regulation to safeguard that right, to the benefit of free and democratic discourse". Article 3 EMFA uses the same language as Article 4 EMFA ("Member States shall…") and its title clarifies that it is a right for the recipients of media services ("Right of recipients of media services")[20]. It is true that Article 3 EMFA in the Commission proposal used more explicit wording ("Recipients of media services in the Union shall have the right…"); however, the change in the formulation of the final text of Article 3 EMFA was done only to avoid the risk of creating an almost boundless obligation for media service providers. It has been objected that Article 3 EMFA does not create a subjective right[21]. However, it is arbitrary to consider, without any objective criterion, that some rights in EMFA are subjective whereas others are objective. Denying the existence of a right for individuals under Article 3 EMFA despite the clear title and the purpose of the provision is untenable in proper legal exegeses. That is underpinned by the systematic argument whereby Article 3 EMFA (like Article 4) specifies the content of the freedom of establishment and the free provision of services under the Treaty, which grant rights to individuals. Furthermore, it cannot be convincingly argued that Article 3 EMFA can be invoked only in combination with another provision of EMFA; in fact, there is no trace of that in the text of EMFA and, moreover, Article 3 EMFA alone entered into application on 8 November 2024, so that its solitary application must have some legal consequences; indeed, in EU law, where different interpretations[22] are possible, the one that preserves the normative value of the provision is to be preferred. What is more, Article 4 EMFA must be read in the light of the fundamental right to freedom of expression and freedom of the press under Article 11 Charter of Fundamental Rights; this provision constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the European Union is founded[23]. In light of the above, it must be considered that paragraph 2 of

18. Italic added.
19. See *ex multis* judgment of 7 February 1979, *Knoors v. Staatssecretaris voor Economische Zaken*, Case 115/78, EU:C:1979:31, § 20.
20. See Malferrari–Gerhold 2024.
21. Cf. Cole–Etteldorf (2024), p. 14. Cf. also Grandinetti 2024, § 5.
22. Cf. the pending case *Viktor Orbàn*, C-384/24.
23. Judgment of 4 October 2024, *Real Madrid v. Le Monde*, C-633/22, EU:C:2024:843, § 49.

Article 4 EMFA, as well as Article 3 EMFA, lay down individual rights proper.

With these clarifications made, it is important to emphasize that Article 4(2) EMFA finds its inspiration in the concept of *Staatsferne* ("distance from the State"). Under the first sentence of Article 4(2) EMFA, "Member States shall respect the *effective* editorial freedom and independence of media service providers in the exercise of their professional activities"[24]. The word "effective" indicates that it is not only the form but also the substance of the editorial freedom and independence that must be respected. This corresponds to a general approach in EU law which focuses on the substance of social and economic phenomena. What follows are the words "in the exercise of their professional activities", which is in keeping with the definition of media service providers, defined as "a natural or legal person whose *professional* activity is to provide a media service…"[25]. The word "professional" limits the definition to those persons who exercise the media activity in a sufficiently deontological and structured manner, thus excluding the improvised or spontaneous journalism that may exist sporadically in particular in the digital society[26]. Thus, the ambit of protected individuals is potentially more limited than those protected under Article 8 ECHR[27]. On the other hand, a profit aim is not necessary to fall into that definition because it is not required under the fundamental freedoms[28].

The second sentence of Article 4(2) EMFA specifies that "Member States, including their national regulatory authorities and bodies, shall not interfere in or try to influence the editorial policies and editorial decisions of media service providers". The term "editorial policies" covers any formal or informal strategy/direction (including guidelines) that a media service provider follows in its professional activity including the content direction of the media offer[29]. Then, the term "editorial decisions" refers to the specific decisions that are taken day-by-day in the exercise of the media profession, including in research, press room activities, investigation, selection, discussion and presentation. They comprise the choice of the topics, the prioritization, the style of presentation, the choice of the presenters and the selection of the guest speakers/writers[30]. According to Article 2, n° 8 of the Commission proposal, "editorial decision" means "a decision taken on a regular basis for the purpose of exercising editorial responsibility and linked to the day-to-day operation of a media service provider". A parallel can be drawn to Article 21 EMFA, whereby national measures that are liable to affect the editorial independence of media service providers can be accepted only under certain conditions. Further, Article 4(2) EMFA finds a pendant in Art. 6(3) EMFA, which protects the journalists' editorial independence and freedom from the media service providers' managers/owners.

The words "interfere in or try to influence" are quite broad, covering any activity that aims at hampering, limiting, affecting or domesticating the media. Indeed, the ways in which the State can, directly or indirectly, actually or potentially, try to exercise any form of influence over the media are varied and sometimes surreptitious[31]. According to recital 18 EMFA, such interference can be direct or indirect, from the State or other actors, including public authorities, elected officials, government

24. Italics added.

25. Italics added. See extensively Verza 2025.

26. For an example cf. judgment of 14 February 2019, *Buivids*, C-345/17, EU:C:2019:122 regarding Mr Buivids's video recording in a station of the Latvian national police and his publishing on Youtube of that video, which showed police officers going about their duties in the police station. In that case the CJEU had to interpret the notion of processing of personal data for journalistic purposes under Article 85 GDPR.

27. Cf. ECtHR's judgment of 8 November 2016, *Magyar Helsinki Bizottság v. Hungary*, n° 18030/11, § 168.

28. Judgment of 23 February 2016, *Commission v. Hungary* ("meal vouchers"), C-179/14, EU:C:2016:108, § 154. But cf. Brogi–Da Costa Leite Borges–Carlini et al. 2023, p. 50.

29. See also Ferreau 2024, p. 41.

30. *Ibidem*.

31. Cf. Trevisan–Štětka–Milosavljevič 2024.

officials and politicians, for example to obtain a political advantage[32]. There is, at the same time, the (legitimate) right of State officials to publicly criticize the work of the media, as long as it is done in a respectful and reasoned manner[33]. The line between the two phenomena may however be thin in practice.

The previous considerations highlight the particular significance of Article 4(2) EMFA. As clarified in the first sentence of recital 17 EMFA, "[t]he protection of editorial independence is a precondition for exercising the activity of media service providers and their professional integrity in a safe media environment. Editorial independence is especially important for media service providers which provide news and current affairs content, given its societal role as a public good". Editorial freedom and independence are essential for the proper functioning of the market and constitute a central feature of the media service: a media service produced without full editorial freedom and independence lacks quality. That is relevant for the internal market, as suggested by the first sentence of recital 16 EMFA which states that "[t]he free flow of trustworthy information is essential in a well-functioning internal market for media services". The State's interference in a media service provider's editorial independence places it at a competitive disadvantage because its services become qualitatively inferior to the services produced by a media service provider which enjoys full editorial independence. Therefore, the fact that a media service provider is - directly or indirectly, actually or potentially - interfered with in the exercise of its economic activity entails a restriction of its economic rights in the internal market and an uneven playing field. As stated in the second sentence of recital 17, "media service providers should be able to exercise their economic activities freely in the internal market and compete on an equal footing in an increasingly online environment where information flows across borders". Editorial freedom and independence of media are of course not only essential elements of the media service, they are also part of the guarantees enshrined in Article 11(2) Charter of Fundamental Rights. The abundant case law of the ECtHR testifies to this. Article 4(2) EMFA is, thus, a good example showing that the economic aspects are inextricably intertwined with the fundamental rights aspects. The previous considerations also play an important role in the debate regarding the legal basis, as is illustrated below.

Article 4 EMFA has been criticized on the ground that the EMFA does not provide for the specifications related to its enforcement[34]. However the details of the enforcement are usually not laid down in the text of regulations or directives, but provided for – as the case may be – in comitology acts; moreover, and in any event, the general clauses laid down in Article 288 TFEU ("A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States") and Article 4(3) TEU ("The Member States shall take any appropriate measure, general or particular, to ensure fulfillment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union") are usually considered to be the sufficient baseline for the obligation of enforcement by Member States[35].

2.3. Article 4(3) and (8) EMFA: the protection of journalistic sources and confidential communications and the right to effective judicial protection

2.3.1. The object of the protection

The protection of journalistic sources and confidential communications is the object of Article 4(3) EMFA whereby "Member State shall ensure that journalistic sources and confidential communications are effectively protected". The structure of the provision is analogue to that of Article 4(2) EMFA. The use of "ensure" underlines that it is an obligation of result for Member States. Member States must take all the legal and practical measures

32. See also Cole–Etteldorf 2023, p. 26.
33. See also Ferreau 2024, p. 42.
34. *Ibidem*.
35. See, to this effect, judgment of 30 March 2023, Case C-34/21, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium*, EU:C:2023:270, § 77.

necessary for the effective protection of journalistic sources and confidential communications. For the same reasons illustrated above as regards Article 4(2) EMFA, this provision too lays down an individual's right. In this context it is to be asked whether the journalistic sources of the individual journalist are protected also *vis-à-vis* the owner of the media organization (in Germany this is called internal media freedom). The wording and the objective of the provision might be insufficient to support an answer in the positive.

The term "journalistic sources" comprises any information on facts and opinions which can be used by media service providers as the basis for a piece of news or an item of journalism. Recital 19 EMFA explains the economic significance of journalistic sources, which "are tantamount to 'raw material' for journalists: they are the basis for the production of media content by journalists, in particular news and current affairs content". As explained in recital 19 EMFA, "[i]t is therefore crucial that journalists' ability to collect, fact-check and analyse information be protected, in particular information imparted or communicated confidentially, both offline and online, which relates to or is capable of identifying journalistic sources". Journalistic sources are often confidential because, either for ethical or professional reasons, some individuals are willing to give information to journalists only under the condition of anonymity or confidentiality. If the anonymity or confidentiality of sources is destroyed, hampered or made less attractive, confidants will be discouraged from providing information to journalists so that the media service providers will have less "raw material" for producing their services, to the detriment of the free exercise of the media service activity.

Recital 21 EMFA emphasizes that the protection of journalistic sources is "crucial for safeguarding the 'public watchdog' role of media service providers, and particularly of investigative journalists, in democratic societies, and for upholding the rule of law". This corresponds to the ECtHR's case law, whereby "[t]he right of journalists to protect their sources is part of the freedom to 'receive and impart information and ideas without interference by public authorities' protected by Article 10 of the Convention and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest"[36]. Without such protection, "the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected"[37]. Not only the publication, but also the preparatory steps to a publication, such as the gathering of information and the research and investigative activities of a journalist are inherent components of the freedom of the press, as enshrined in Article 10 of that Convention, and are, as such, protected[38]. In light of this case law and given the objective of Article 4(3) EMFA, the expression "journalistic sources" is to be interpreted broadly[39]. Indeed, in order to take account of the importance of the freedom of the press and the freedom of expression in media in every democratic society, it is necessary to interpret broadly concepts related to those freedoms[40].

The term "confidential communications" refers to any communication that because of its content or origin is imparted in a reserved manner and plays a role in the production/distribution of media content. Here again, given the liberal objective of the provision, this term is to be interpreted broadly.

Under Article 4(3) EMFA, the protection against State intervention is extended to persons who, because of their regular or professional relationship with a media service provider or its editorial staff,

36. ECtHR, judgment of 14 September 2010, *Sanoma Uitgevers B.V. v. the Netherlands*, Application n° 38224/03, § 50.
37. ECtHR, judgments of 27 March 1996, *Goodwin v. the United Kingdom*, Application n° 17488/90, § 39; of 29 June 2006, *Weber and Saravia v. Germany (dec.)*, Application n° 54934/00, § 143.
38. Judgment of 15 March 2022, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, § 68, with reference to ECtHR, judgments of 25 April 2006, *Dammann v. Switzerland*, § 52, and of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, § 128.
39. See also Ferreau 2024, p. 43.
40. *Autorité des marchés financiers*, cit., § 66.

might have relevant information[41]. This category is defined functionally, and, in view of its rationale, it is also to be interpreted broadly[42].

2.3.2. Three specific prohibitions for Member States

The second sentence of Article 4(3) EMFA specifies three types of measures which Member States shall not take. These three types of measures constitute restrictions to the free exercise of the media service provider activity. They are as follows:

a) to oblige media service providers or their editorial staff to disclose information related to or capable of identifying journalistic sources or confidential communications;
b) to detain, sanction, intercept or inspect media service providers or their editorial staff or subject them to surveillance or search and seizure;
c) to deploy intrusive surveillance software on media service providers.

The channels of communications between journalists and sources can thrive thanks to the digitalization, but are at the same time subject to new and invasive threats which are increasingly cross-border[43]. A risk for journalistic sources and confidential communications is particularly strong where, as is typically the case for spyware, the data are collected without the persons concerned being informed[44]. Going beyond this scenario, any risk, even of potential or indirect nature, for the sources or confidential communications is liable to lead to a chilling effect for the media[45]. Therefore, these three categories of prohibitions are to be construed broadly, i.e., rigorously. Orders to disclose sources potentially have a detrimental impact, not only on the source itself, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources, and on members of the public, who have an interest in receiving information imparted through anonymous sources[46]. It is irrelevant whether the media service providers are unaware of any detainment, sanction, interception or inspection taking place, because the condition of awareness is not laid down[47]. It is equally irrelevant whether the media service providers refuse disclosure or not because the potential negative effect on sources remains.

2.3.3. Derogation from the prohibitions under (strict) conditions

State intervention is, however, allowed under certain detailed conditions which are set out in the following paragraphs of Article 4 (i.e., paragraphs 4 and 5). According to Article 4(4) EMFA, one of the national measures listed above can be accepted only if it is:

a) provided for by Union or national law ("legality principle");
b) in compliance with Article 52(1) of the Charter and other Union law;
c) justified on a case-by-case basis by an overriding reason of public interest and proportionate;
d) subject to prior authorization by a judicial authority or an independent and impartial decision-making authority or, in duly justified exceptional and urgent cases, is subsequently authorized by such an authority without undue delay.

As regards the deployment of intrusive surveillance software (in short: spyware) referred to in point c) of Article 4(3) EMFA, two additional conditions for the derogation are laid down in paragraph 5 of Article 4 EMFA as follows:

– the measure is carried out for the purpose of investigating one of the persons referred to in paragraph 3, point (c), with regard to:

41. See also recital 20 EMFA.
42. See to this effect Ferreau 2024, p. 45.
43. Cf. Gerhardinger 2023, Section II.
44. See, by analogy, judgment of 21 December 2016, *Tele 2 Sverige and Watson*, joined cases C-203/15 and C-698/15, EU:C:2016:970, § 100.
45. Woodhams 2021, p. 18.
46. *Sanoma*, cit., § 89.
47. Voorhoof 2022, p. 3.

(i) offences listed in Article 2(2) of Framework Decision 2002/584/JHA punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least three years; or
(ii) other serious crimes punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least five years, as determined by the law of that Member State;

– one of the measures mentioned under points a) or b) would not be adequate and sufficient ("*ultima ratio*" or "subsidiarity rule").

Exceptions to rules are to be construed narrowly so that general rules are not negated[48]. In addition, according to the settled case-law of the ECtHR, exceptions to the freedom of expression are to be construed strictly and Article 10(2) ECHR leaves little scope for restrictions on freedom of expression in the fields of political speech and matters of public interest[49]. Therefore, all the abovementioned conditions shall be construed rigorously. As remarked by the Venice Commission, "[w]ith particular regard to journalism, it is well-established that surveillance tools may be applied in only the most exceptional circumstances. European and international sources have widely recognized that journalism's watchdog role requires exceptional caution when considering interferences with their functions"[50].

2.3.4. The derogation as codification of case law guarantees

By and large, the abovementioned conditions codify in substance the application of the general principles of EU law and/or existing rules under the ECHR, which are relevant pursuant to the synchronization provision laid down in Article 52(3) Charter. So, for example, the legality principle under letter a) entails that the legal basis authorizing the interference must define its scope and all the constituent elements sufficiently clearly and precisely[51]. Then, as regards the *ultima ratio* (or subsidiarity) rule laid down in Article 4(5) EMFA, under the case law of the ECtHR, if a Member State wishes to use intrusive surveillance software, it must be able to demonstrate that it is strictly necessary[52] and there are no less intrusive surveillance methods available to achieve the aim pursued[53]. The last part of Article 4(5) EMFA thus has the added value of clarifying and specifying the ambit of application of those principles and rules. Moreover, they make the guarantees applicable even in a purely domestic scenario, whereas the fundamental freedoms apply only in the presence of a cross-border element. In this context it should be added that the *ultima ratio* condition is part of the proportionality principle, which being a general principle of EU law applies to the whole of Article 4(3-5) EMFA. This means that searches and confiscations or other surveillance measures are unlawful if less intrusive measures are adequate and sufficient.

The obligation of prior authorization under Article 4(4)(c) EMFA, which was introduced during the negotiations, is particularly important in practice because it introduces the verification by an independent organ. Its absence in the Commission proposal was considered to be a lacuna because the obligation of prior authorization is a guarantee already provided for under Article 10 ECHR[54]. The ECtHR has indeed emphasized the importance of prior authorization by an independent organ for

48. Judgment of 28 October 2022, *HF and Generalstaatsanwaltschaft München*, C-435/22 PPU, EU:C:2022:852, § 120.
49. *Real Madrid v. Le Monde*, cit., § 53.
50. Venice Commission 2024, § 93.
51. See to this effect and by analogy *CG Bezirkshauptmannschaft Landeck*, cit., § 98 regarding the Law Enforcement Directive.
52. ECtHR, judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 73, and judgment of 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, C-73/07, EU:C:2008:727, § 56; of 9 November 2010, *Volker und Markus Schecke*, joined cases C-92/09 and C-93/09, EU:C:2010:662, § 77.
53. See, by analogy, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, § 53.
54. See also Voorhoof 2022, p. 5.

interceptions of journalists[55]. The extension of the power of prior authorization to other independent authorities has been criticized on the grounds that they lack the same level of independence as the judicial branch, as they are part of the administrative branch of the executive power[56]. This criticism should be taken seriously; indeed, the ECtHR in *Sanoma* considered the public prosecutor's authorization to be incompatible with Article 10 ECHR because he/she was too much involved in the investigation and there was no pertinent authorization by an investigating judge[57]. But this criticism needs, at the same time, to be nuanced because in *Sanoma v. the Netherlands* the ECtHR found that the Member State involved (the Netherlands) had violated Article 10 ECHR inter alia on the ground that under the relevant Dutch legislation in terms of procedure the public prosecutor is a "party" defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests[58]. A sufficient level of independence is instead required by Article 4(4)(c) EMFA. Indeed, that provision is to be construed in view of its protective objective and in consonance with the fundamental rights. This also finds expression in recital 21 EMFA, whereby "[i]n light thereof, ensuring an adequate level of protection for journalistic sources and confidential communications requires that measures for obtaining such information be authorised by an authority that can independently and impartially assess whether it is justified by an overriding reason of public interest, such as a court, a judge, a prosecutor acting in a judicial capacity, or another such authority with competence to authorise those measures in accordance with national law". The expression "another such authority" indicates that the authorities that may authorize the use of the restrictive measures at issue must have a level of independence and impartiality that is analogue to that possessed by a judicial organ. The prior authorization can be dispensed of only "in duly justified exceptional and urgent cases". The justification and urgency must be validly established before that exception can be used[59]. In any event it must remain exceptional.

2.3.5. The obligation of regular review of restrictive measures

Paragraph 6 of Article 4 EMFA further specifies that the abovementioned measures under b) and c) of Article 4(4) EMFA must be regularly reviewed in order to verify whether the conditions are still being met. This also corresponds in substance to the guarantees existing under the ECHR[60]. Given its purpose, it must be interpreted rigorously. It is an important provision in practice because otherwise the risk of overly long duration of the restrictive measures would be tangible.

2.3.6. The applicability of the Law Enforcement Directive

Paragraph 7 of Article 4 EMFA provides that the Law Enforcement Directive "shall apply to any processing of personal data carried out in the context of the deployment of the surveillance measures referred to in paragraph 3, point (b), of this Article or the deployment of intrusive surveillance software referred to in point (c) of that paragraph". It is unclear what the legal value of this provision is[61]. It could be asked whether it is purely declaratory in nature despite the use of the verb "shall". Indeed, pursuant to Article 1(1), the Law Enforcement Directive "lays down the rules relating to the protection of natural persons with regard to the processing of personal data by

55. Judgments of the ECtHR of 25 May 2021, *Big Brother Watch v. UK*, Applications nos. 58170/13, 62322/14 and 24960/15), §§ 351 et seq.; of 28 November 2024, *Klaudia Csikós v. Hungary*, Application n° 31091/16, §§ 53-54. See Voorhoof 2021; Voorhoof 2025.

56. Bayer 2024, p. 122.

57. ECtHR, judgment of 14 September 2014, *Sanoma v. the Netherlands*, Application n° 38224/03, § 100. See also Kermer 2024, p. 198.

58. *Sanoma*, cit., § 93.

59. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 120.

60. See to this effect ECtHR, judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 26.

61. See also Ferreau 2024, p. 54.

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". That said, the insertion of paragraph 7 of Article 4 EMFA may be explained by the legal uncertainty regarding the exact ambit of application of the Law Enforcement Directive. Such uncertainty stems in particular from the rather ambiguous recital 14 of that Directive, whereby "[s]ince this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive". This recital is of course to be read together with other parts of the Law Enforcement Directive such as Articles 13(3), 15(1) and 16(4), which indicate that Member State measures related to national security may fall into the ambit of application of the Directive[62]. Therefore, the legal uncertainty regarding the Directive was more perceived than real.

2.3.7. Judicial remedies and supportive independent authority/body

Paragraph 8 of Article 4 EMFA, in its first part, is about the remedies for media service providers. It has a declaratory nature, restating what already flows from Article 47 Charter of Fundamental Rights of the EU. Then, the second part of paragraph 8 of Article 4 EMFA provides that "Member States shall entrust an independent authority or body with relevant expertise to provide assistance to the persons referred to in the first subparagraph with regard to the exercise of that right". This authority/body will play an important role in upholding the rights of media service providers, as will be illustrated in detail below. The provision further specifies that "[w]here no such authority or body exists, those persons may seek assistance from a self-regulatory body or mechanism". This latter specification is a novelty in the provision because the words "shall entrust" in the previous sentence of Article 4(8) EMFA lay down an obligation and not an option for Member States to have in place an independent authority or body with relevant expertise. Legal provisions usually start from the premise that Member States comply with EU legal obligations, *a fortiori* where the obligation in question is laid down in the same legislative act. The sentence starting with "where no such authority exists" seems, by contrast, to explain what individuals can do in the event that the Member State concerned fails to comply with the abovementioned obligation to entrust an independent authority or body to provide assistance. The words "may seek assistance" could be construed as bestowing an individual's right upon the persons concerned.

2.4. The national security dispute

Paragraph 9 of Article 4 EMFA states, as already anticipated above, that "[t]he Member States' responsibilities as laid down in the TEU and the TFEU are respected". This terse provision is, as follows from recital 8, *in fine*, of the EMFA, a purely declaratory statement: it contains a mere description of what Article 4(2) TEU already does. Indeed, under this provision of the Treaty, "[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State".

Behind the very succinct wording of Article 4(9) EMFA lies a hard-fought debate in which two opposing camps were involved: on the one hand, the sovereigntists led by the French Ministry of Defense, which advocated for an outright carve-out in favor of national security[63], and, on the other hand, the journalist associations and NGOs,

62. See also by analogy *Tele 2 Sverige and Watson*, cit.

63. See *RSF urges French Interior Minister to abandon the national security exception in European Media Freedom Act* and *Hardline EU governments in late push to legitimise surveillance of journalists*.

which vehemently opposed any mention whatsoever of Member State powers in this field[64]. In the end, common sense has prevailed: a carve-out in favor of national security has been rejected because it would have deprived the whole Article 4(3) EMFA largely of any legal meaning and would have probably collided with the ECtHR's case law[65]. At the same time, there is a mention of the State powers albeit an innocuous one because it merely reiterates the content of Article 4(2) TEU[66]. In that regard, it corresponds to the solution chosen by the legislator in the NIS2 Directive[67] and starkly contrasts with the ominous recital imposed by the Council of the European Union in the AI Act, which has been rejected by the Commission in a declaration[68].

Article 4(2) TEU indicates that in the essential State functions of Member States, it is their exclusive responsibility to safeguard national security. The wording, purpose and context of the provision indicate that Article 4(2) TEU has a framing function and does not entail an exception to the application of EU law[69]. The CJEU held in the judgment *La Quadrature du Net* that "according to the Court's settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law"[70]. Although it is for the Member States to adopt appropriate measures to ensure law and order on their territory and their internal and external security, it does not follow that such measures *per se* fall outside the scope of European Union law. As the CJEU has held, "the only articles in which the FEU Treaty expressly provides for derogations applicable in situations which may affect law and order or public security are Articles 36, 45, 52, 65, 72, 346 and 347, which deal with exceptional and clearly defined cases. It cannot be inferred that the FEU Treaty contains an inherent general exception excluding all measures taken for reasons of law and order or public security from the scope of European Union law. The recognition of the existence of such an exception, regardless of the specific requirements laid down by the Treaty, might impair the binding nature of European Union law and its uniform application"[71]. This position is fully in line with previous case law from which the drafters of Article 4(2) TEU drew inspiration[72]. Therefore, measures adopted by Member States to safeguard national security, defense and public security are not, as such, excluded from the application of EU law solely because they are presented as being taken in the interest of national

64. As regards the various sources see Bayer 2024, p. 123.

65. See *Big Brother Watch v. UK*, cit.

66. See also, to this effect, Ferreau 2024, p. 53. But cf. Kermer 2024, p. 200.

67. Art. 2(6) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

68. Recital 24 of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

69. See Opinion of AG D. Spielman in Case C-448/23, *Commission v. Poland* ("judgments of the Polish Const. Court"), EU:C:2025:165, §§ 67-69 and 85-88.

70. Judgment of 6 October 2020, *La Quadrature du Net 1*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, § 99.

71. Judgment of 17 December 2020, *Commission v. Hungary* ("reception of applicants for international protection"), C-808/18, EU:C:2020:1029, § 214.

72. See, for example, judgments of 9 December 1997, *Commission v. France* ("Spanish strawberries"), C-265/95, EU:C:1997:595, §§ 33 to 35; of 11 January 2000, *Tanja Kreil v. Germany*, C-285/98, EU:C:2000:2, §§ 16 to 17; of 11 March 2003, *Alexander Dory v. Germany*, C-186/01, EU:C:2003:146, § 30; 8 April 2008, *Commission v. Italy* ("helicopters"), C-337/05, EU:C:2008:203, §§ 42-43; of 20 March 2018, *Commission v. Austria* ("State printing office"), C-187/16, EU:C:2018:194, §§ 75 to 78.

security[73]. In other words, national security is not a blank cheque that can be invoked by Member States to escape from their obligations under EU law[74]. Member States must comply with EU law even where they exercise an exclusive competence.

When taking measures to safeguard national security, Member States must be able to demonstrate, on the basis of sufficiently solid grounds, that they are confronted with a serious threat to national security which is shown to be genuine and present or foreseeable[75]. A Member State which wishes to avail itself of the derogations for the protection of its essential security interests must show that such a derogation is necessary in order to protect those interests[76]. It is for the Member State concerned to demonstrate these conditions, in particular that justification and proportionality are met. As regards, specifically, the condition that the provisions restricting internal market freedoms must be justified by one of the reasons listed in the Treaty or by an overriding reason in the public interest, it must be recalled that Member States must prove, in a concrete manner and by reference to the circumstances of the case, that those provisions are justified[77]. The ECHR imposes analogue limits to the use of security interests as a derogation to human rights[78].

The net result is that it is only under these conditions that Member States will be able to invoke national security to justify a derogation to the prohibition laid down in Article 4(3) EMFA; moreover, Member States will need to prove in a concrete, detailed and circumscribed manner with regard to the circumstances of the case that the conditions set out in paragraphs 4 and 5 of Article 4 EMFA are fulfilled and that the fundamental rights and the general principles of EU law (such as legal certainty and proportionality) are complied with.

2.5. Regulating spyware as the "major novum" under Art. 4 EMFA

It is worthwhile zooming in on spyware. Spyware comprises several types: for example, "underground spyware", commercially available spyware, and spyware developed by public authorities. In any form, spyware is one of the nightmares of privacy defenders; it has even been compared – not without ground – to a weapon[79]. From the opposite angle, it is a phenomenal investigative tool in the hands of public and private entities. Whereas the Commission's proposal used the term "spyware" as one of the defined terms, the final version of EMFA has preferred to use the term "intrusive surveillance software", which means "any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, including in an indiscriminate manner" (Article 2 n° 20 EMFA). The definition set out in the final version of the EMFA is arguably broader than the one in the Commission's proposal[80]. Indeed, it notably leaves out the terms "in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent in that regard". The definition in Article 2 n° 20 EMFA protects any type of data, including encrypted ones.

73. See in particular the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)); Mildebrath 2022, p. 41.
74. But see, although without argumentation, Ferreau 2024, p. 54.
75. See, to this effect, *La Quadrature du Net 1*, cit., § 137.
76. *Commission v. Austria* ("State printing office"), cit., § 78.
77. Judgment of 18 June 2020, *Commission v. Hungary* ("NGOs"), C-78/18, EU:C:2020:476, § 77.
78. European Court of Human Rights 2022, pp. 61-65.
79. Phillips 2023, p. 5.
80. Kermer 2024, pp. 198-199.

The spyware matter has been brought to the attention of public opinion, inter alia, through several scandals including the so-called Pegasus scandal from 2021, referring to the notorious software "Pegasus" produced by the Israel-based NOS group[81]. Several opinions, reports, debates, studies and recommendations have followed[82]. On 16 October 2023 the Parliamentary Assembly of the Council of Europe declared in a resolution that the secret surveillance of political opponents, public officials, journalists, human rights defenders and civil society for purposes other than those listed in the European Convention of Human Rights, such as preventing crime or protecting national security, would be a clear violation of the Convention. According to the Venice Commission of the Council of Europe, "the potential for unjustified or disproportionate intrusive surveillance using such a tool is significant. If left unregulated, spyware is a potent surveillance weapon that can be used to curtail human rights, censor and criminalise criticism and dissent and harass (or even suppress) journalists, human rights activists, political opponents and repress civil society organisations"[83]. It further held that "[t]he Pegasus scandal showed that journalists were apparently being targeted simply because they are journalists, which is unacceptable in a democratic society"[84]. Substantial forensic reporting by civil society organizations – such as Citizen Lab, Amnesty Tech, and AccessNow – has identified significant evidence of abusive surveillance using spyware technologies[85].

There are two extraordinary things about spyware. First, its pervasiveness and sophistication: as Bill Marczak of Citizens Lab recalled during his testimony at the PEGA Committee of the European Parliament, spyware is not only a tool for listening in and abducting data, but is also capable of doctoring documents, changing preferences of the device and activating tools of the targeted device such as the camera or other apps. Second, its ease of use is remarkable: Bill Marczak explained that, once you buy a license to use Pegasus for a specific country, you merely need to dial in the telephone number you want to target, and that is sufficient to put it under surveillance (so-called "zero-click spyware"). As noted by the Venice Commission, "technical developments make surveillance 'easier and easier to use'"[86]. Spyware yields thus an unprecedented level of intrusion thanks to its powerful technological sophistication. Spyware such as Pegasus should not be equated with "traditional" law enforcement interception tools; rather, it appears to be more similar to "government Trojan" or "online searches" solutions that had in the past raised serious legal concerns[87].

Accordingly, the use of spyware constitutes a major challenge to the rule of law, fundamental rights and values of the EU, which "define the very identity of the European Union as a common legal order"[88]. That is particularly true for the media. As clarified in recital 25 EMFA, intrusive surveillance software "has dissuasive effects on the free exercise of economic activities in the media sector. It jeopardises, in particular, the trusted relationship of journalists with their sources, which is the core of the journalistic profession. Given the digital and intrusive nature of such software and the use of devices across borders, it has a particularly detrimental impact on the exercise of economic activities by media service providers in the internal market. It is therefore necessary to ensure that media service providers, including journalists, operating in the internal market for media services can rely on robust harmonised protection in relation to the deployment of intrusive surveillance software in the Union, including where Member State authorities resort to private parties to deploy

81. See Mildebrath 2022, p. 41; Kermer 2024-a. See also Reuters 2025.

82. For a list see Venice Commission 2024, §§ 31-33. See also Vidal Marti 2023.

83. Venice Commission 2024, § 12.

84. *Ivi*, § 96.

85. *Ivi*, § 12.

86. *Ivi*, § 14.

87. European Data Protection Supervisor 2022, p. 4.

88. Judgment of 16 February 2022, *Hungary v. EP and Council* ("Conditionality Reg."), C-156/21, EU:C:2022:97, § 127.

it"[89]. This is also relevant for the issue of legal basis, which is discussed below.

That said, we live in a world where criminal threats are challenging and increasingly sophisticated. Spyware can be used by law enforcement authorities to put nefarious and technically adept criminals under surveillance. This can be done also cross-border through the cooperation of authorities from different Member States: an example thereof can be drawn from the Case C-670/22, *Staatsanwaltschaft Berlin v. M.N.* Thus, spyware can also be used to benefit legitimate societal goals. Indeed, Member States have a national security responsibility under Article 4(2) TEU and a competence for the maintenance of law and order (cf. Article 72 TFEU).

The balancing of these conflicting needs is a very delicate exercise, which the legislator has achieved in Article 4 EMFA. It is the result of the confrontation between two opposing camps which emerged in the legislative process of the EMFA with regard to Article 4. Whereas the European Parliament pushed for far-reaching protection against intrusive surveillance software, the Council (in particular some Member States) had a more cautious approach[90]. The solution adopted by the EU legislator in Article 4 EMFA strikes a good balance, by relying in substance on the guarantees provided by the Charter of fundamental rights of the EU, the general principles of EU law, the ECHR and the Convention 108[91]. EMFA, thus, needs to be put into the context of the already existing fundamental rights guarantees and general principles of EU law.

In its case law, the ECtHR has worked out a number of guarantees to protect individuals from secret surveillance by the State, such as: the State's obligation to set out the circumstances and the conditions upon which public authorities may resort to surveillance measures; the obligation to define the categories of individuals who can be subject to surveillance; the obligation to set a limit on the duration of surveillance; the obligation to determine the procedure that needs to be complied with when examining, using, and storing the data obtained; the obligation to take precautions when communicating the data to other parties; the obligation to specify the circumstances under which the obtained data must be erased or destroyed[92].

The list of crimes that is set out in Article 4(5)(b)(ii) EMFA, which has been criticized for being excessively broad[93], raises an issue which however must be relativized in its practical consequences because that provision must be interpreted in compliance with the EU fundamental rights and the general principles of EU law. Under the CJEU's case law, in compliance with the principles of necessity and proportionality, the seriousness of the intrusion can be justified only by the seriousness of the public interest that is pursued by the public authorities[94]. This corresponds in substance to the ECtHR's case law[95], whereby the higher the level of interference, the more robust the level of safeguards must be[96]. In *La Quadrature du Net II*, the CJEU used the terms "serious and even 'particularly serious' interferences with the fundamental rights concerned" when referring to national measures allowing general access to all retained traffic and

89. See also ECtHR, decision of 8 December 2005, *Nordisk Film & TV A/S v. Denmark*, Application n° 40485/02; *Sanoma*, cit., § 65.

90. See Ferreau 2024, p. 51.

91. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n° 108, 2018).

92. ECtHR, judgments of 24 April 1990, *Huvig v. France*, Application n° 11105/84, § 34; of 29 June 2006, *Weber and Saravia v. Germany (dec.)*, Application n° 54934/00, § 95; and of 11 January 2022, *Association for European Integration and Human Rights and Ekimdzhiev and Others v. Bulgaria*, Application n° 70078/12, § 76.

93. Kermer 2024, p. 202.

94. *La Quadrature du Net II*, cit., 95. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 102.

95. See, to this effect, Ferreau 2024, p. 47.

96. Judgments of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, §§ 116-117; of 8 December 2022, *Orde van Vlaamse Balies*, C-694/20, EU:C:2022:963, § 41.

location data[97]. The seriousness of the offence is one of the main parameters in assessing the proportionality of the interference that accessing the personal data contained in a mobile telephone represents[98]. In light of the findings made by the PEGA Committee of the European Parliament and of the abovementioned report by the Venice Commission[99], the interference with fundamental rights by spyware is usually extremely serious[100]; that is all the more so that it cannot be ruled out that the data contained in a device such as a mobile phone may include particularly sensitive data[101]. The corollary is that the public interest that needs to be invoked to justify the use of spyware must also be very serious, i.e., that the seriousness of the offence pursued must be particularly high, accordingly. It is true that the CJEU, when interpreting the Law Enforcement Directive, held that to consider that only combatting serious crime may justify access to data contained in a mobile telephone would limit the investigative power of the competent authorities and that would increase the risk of impunity of such offences[102]. However, that judgment was handed down in a case regarding a "normal" access to a phone data and not access through spyware. Moreover, the judicial dictum regarding the correspondence between the seriousness of the intrusion and the seriousness of the objective pursued belongs to settled case law of the CJEU. It follows that the Member States cannot distort the concept of "serious offence" and, by extension, that of "serious crime", by including within it, for the purposes of applying the derogation under Article 4(5) EMFA, offences which are manifestly not serious offences, in the light of the societal conditions prevailing in the Member State concerned, even though the legislature of that Member State has provided for such offences to be punishable by a maximum term of imprisonment of five years[103]. Moreover, the fact that a journalist's conduct falls into the category of the crimes listed in Article 4 EMFA is alone insufficient to justify the deployment of spyware; in fact, additional requirements must be fulfilled, including proportionality in concreto (see below), so that judicial or independent authorities must refuse the authorization of the restrictive measure if the offence at issue is manifestly not serious[104].

The obligation of justification entails that Member State authorities must prove that the use of spyware is justified by an overriding reason of public interest with regard to one of the crimes listed in Article 4(5) EMFA. The terms "overriding reason of public interest" is an EU law concept, so that Member States authorities cannot define it *ad libitum*: they can invoke it only where the public interest is sufficiently clearly defined and fulfills the criteria set out in the EU case law. In view of the wording in the German version of Article 4(4) (c) EMFA, the opinion has been expressed that this provision requires a mere balancing of the different interests and not a strict necessity examination[105]. It is, however, not clear whether the German version would imply a more lenient verification of the justification requirement. Moreover, and in any event, this opinion overlooks the fact that other versions such as the English, French, Italian and Spanish ones use the usual expression ("overriding reasons of public interest", "raisons impérieuses d'interêt général", "motivo imperativo

97. Judgment of 30 April 2024, *La Quadrature du Net II*, Case C-470/21, EU:C:2024:370, § 128.

98. See, by analogy, judgment of 4 October 2024, *CG v. Bezirkshauptmannschaft Landeck*, C-548/21, EU:C:2024:830, § 96 regarding the Law Enforcement Directive.

99. Venice Commission 2024, § 9. See also European Data Protection Supervisor 2022, p. 8 whereby "[t]he level of interference with the right to privacy is so severe that the individual is in fact deprived of it".

100. *Tele 2 Sverige and Watson*, cit., § 100.

101. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., §§ 94-95 and 107 regarding the Law Enforcement Directive.

102. *CG v. Bezirkshauptmannschaft Landeck*, cit., § 97.

103. See, by analogy, judgment of 30 April 2024, *Procura di Bolzano*, C-178/22, EU:C:2024:371, § 50.

104. See, by analogy, *Procura di Bolzano*, cit., § 62. See also, to this effect and by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 105 regarding the Law Enforcement Directive. See Palmiotto 2024.

105. Ferreau 2024, p. 46.

d'interesse generale" and "una razón imperiosa de interés general") which is also used in other pieces of EU legislation (e.g., the Services Directive) as well as in the CJEU's case law regarding the justification of restrictions to free movement under the Treaty. In addition, the principle of proportionality, being a general principle of EU law, applies in the context of the application of secondary law such as Article 4(4)(c) EMFA. It must also be understood in accordance with the concept/condition of "an overriding requirement in the public interest" and the inherent (procedural) guarantees as developed in the case law of the ECtHR on the protection of journalistic sources. Therefore, it is well-founded to consider that a full justification and necessity examination must be conducted under Article 4(4)(c) EMFA. In that regard, the measure adopted must correspond genuinely and strictly to the objective of investigation set out in Article 4(5) EMFA[106]. The Member State must prove in a concrete manner and by reference to the circumstances of the case, that the measure is justified[107]. Therefore, it cannot be validly considered that the EU legislator has *en bloc* justified or even blessed the use of spyware by national authorities. The compliance with Article 4 EMFA of the use of spyware depends on a number of strict conditions which must be proved according to the burden of proof set out in EU law: it is only under the proviso that the use of spyware, in a specific case (not *en bloc*!) may possibly be compatible with the EMFA. In particular, politically motivated surveillance is certainly incompatible with Article 4 EMFA because it does not qualify as a valid justification.

In this context it must be emphasized that the test of proportionality, which is a general principle of EU law and whose observance is recalled in Art. 4(4) EMFA, plays a very important (often crucial) role in practice. In accordance with that principle, the surveillance measure, including its duration and scope, shall not exceed what is necessary to achieve the (legitimate) objective pursued[108]. This requires balancing, on the one hand, the need to combat one of the serious crimes listed in Article 4(5) EMFA and, on the other hand, the seriousness of the interference with an individual's right to data protection and private life[109]. Recital 26 EMFA, by relying on the case law, explains in detail what the principle of proportionality entails. It states that "[a]ccording to the principle of proportionality, limitations can be made to an individual's rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union. Thus, as regards specifically the deployment of intrusive surveillance software, it is necessary to ascertain whether the offence in question attains a threshold of seriousness as laid down in this Regulation, whether, following an individual assessment of all the relevant circumstances in a given case, the investigation and prosecution of that offence merit the particularly intrusive interference with fundamental rights and economic freedoms consisting in the deployment of intrusive surveillance software, whether there is sufficient evidence that the offence in question has been committed, and whether the deployment of intrusive surveillance software is relevant for the purpose of establishing the facts related to the investigation and prosecution of that offence"[110]. This constitutes detailed and precious guidance for the national authorities, in particular the judiciary, in the application of Art. 4 EMFA.

When interpreting secondary law such as Article 4 EMFA, national authorities must take account of the fundamental rights such as liberty and security, private and family life, privacy, free-

106. See, by analogy, *La Quadrature du Net II*, cit., § 67 as regards Article 15(1) of Directive 2002/58.

107. Judgments of 18 June 2020, *Commission v. Hungary* ("usufruct"), C-235/17, EU:C:2020:476, § 77; *Commission v. Hungary* ("NGOs"), cit., § 77.

108. See also Article 5 of Convention 108 and ECtHR, judgment of 2 September 2010, *Uzun v. Germany*, Application n° 35623/05. The ECtHR found that a GPS device for location tracking was a less intrusive measure than the interception of personal communications.

109. See, by analogy, *La Quadrature du Net I*, cit., § 131.

110. As regards the need for evidence, in the context of the interpretation of Law Enforcement Directive the CJEU has required the existence of reasonable suspicions is supported by subjective and sufficient evidence (*CG v. Bezirkshauptmannschaft Landeck*, cit., § 101).

dom of expression, and freedom and pluralism of the media, enshrined respectively in Articles 6, 7, 8, 11(1) and 11(2) Charter of the fundamental rights of the EU[111]. The interpretation of relevant secondary law must take account of the importance of the right to freedom of expression, which constitutes one of the essential foundations of a pluralistic, democratic society, and is one of the values upon which, under Article 2 TEU, the Union is founded[112]. Spyware interferes not only with freedom of expression and freedom of the media, but also with the rights of both journalists and third parties to privacy and to private life; this reinforces the need for a particularly limited use of such measures and the requirement of very precisely developed provisions[113]. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 ECHR[114]. The protection of the fundamental right to respect for private life at EU level requires that derogations and limitations on the protection of personal data are to apply only in so far as is strictly necessary[115]. The ECtHR specified that the right to privacy would be "unacceptably weakened if the use of modern technologies in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests"[116]. The particular context in which the interference with fundamental rights takes place, in particular the modalities of the intrusion and the amount of data obtained, cannot be ignored in the analysis[117]. One of the findings in the interesting report published in April 2023 by the UN Human Rights Council and drafted by special rapporteur Prof. Fionnuala Ní Aoláin of the University of Minnesota Law School is that there may well be a category of spyware which, by virtue of its indiscriminate and disproportionate impact, can never be operated in a lawful manner[118]. It can be inferred from Article 11 Charter of Fundamental Rights a positive obligation for Member States to avoid lacunae in the security of IT systems concerned, just like Member States are pursuant to Article 10 ECHR under a positive duty to set up a legal framework to ensure effective media pluralism[119].

A further general principle of EU law is legal certainty. According to that principle, individuals must have access to the relevant legal rules (including those governing the use of surveillance measures) and must be able to anticipate the consequences of their application[120]. The law must indicate the limits to discretion conferred on the authorities and the criteria according to which it is exercised with sufficient clarity in order to give to individuals adequate protection against arbitrary interference[121]. The principle of legal certainty requires that EU or national rules are clear, precise

111. See, by analogy, *La Quadrature du Net II*, cit., § 68.

112. See, to this effect, *La Quadrature du Net II*, § 68.

113. Cf. Cole–Etteldorf 2023, p. 28.

114. ECtHR, judgment of 4 December 2008, *S. and Marper v. the United Kingdom*, Applications n° 30562/04 and 30566/04, § 103.

115. *Tele 2 Sverige and Watson*, cit., § 96.

116. ECtHR, Judgment of 13 February 2023, *Podchasov v. Russia*, Application n° 33696/19, § 62.

117. See, by analogy, *La Quadrature du Net II*, cit., § 107 as regards Article 15(1) of Directive 2002/58.

118. Ní Aoláin 2023.

119. ECtHR, judgment of 7 June 2012, *Centro Europa 7*, application n° 38433/09, § 134. See also, by analogy, Order by the German Constitutional Court of 8 June 2021, *1 BvR 2771/18*, § 32.

120. See, to this effect, judgment of 10 March 2009, *Proceedings brought by Heinrich*, C-345/06, EU:C:2009:140, § 44. ECtHR, judgments of 18 May 2010, *Kennedy v. the United Kingdom*, Application n° 26839/05, § 151 of 4 May 2000, *Rotaru v. Romania*, Application n° 28341/95, § 52; of 1 July 2008, *Liberty and Others v. UK*, Application n° 58243/00, § 59; and of 10 February 2009, *Iordachi and Others v. Moldova*, Application n° 25198/02, § 37.

121. See, to this effect, judgment of 4 June 2002, *Commission v. France* ("Elf-Aquitaine"), C-483/99, EU:C:2002:327 § 50; ECtHR, judgments of 6 December 2007, *Liu v. Russia*, Application n° 58149/09, §§ 92 and 98; of 4

and predictable as regards their effects, in particular when they may have unfavorable consequences for private individuals and undertakings[122]. When public authorities act within the scope of EU law, they must exercise their discretion on the basis of objective, non-discriminatory, sufficiently specific and clear criteria known in advance[123].

Under Article 4(5)(b) EMFA, the deployment of spyware must be carried out "for the purpose of investigating one of the persons referred to in paragraph 3, point (c)". This wording indicates that spyware can be used against a given target only to investigate a crime that has been likely committed by him/her and not by other individuals[124]. This interpretation is also in line with the objective of the provision, which is to offer a "robust harmonized protection in relation to the deployment of intrusive surveillance software in the Union" (recital 19 EMFA), and with the fundamental rights of journalists.

The secret nature of surveillance serves, to a certain extent, a functional purpose in the investigations, but collides with an individual's rights such as the right of defence. The right for individuals to be notified that they were subject to the use of surveillance is recognized in the case law as being instrumental to enable the affected individuals to exercise their right to the protection of personal data and to privacy as well as their right to an effective judicial remedy[125]. This is recognized in recital 22 of EMFA whereby "in line with the established case law of the European Court of Human Rights, the right to effective judicial protection presupposes, in principle, being informed in due time, without jeopardising the effectiveness of ongoing investigations, of the surveillance measures taken without the knowledge of the person concerned in order to effectively exercise that right"[126]. The limitations of the right to notification in due time must be provided for by law, respect the essence of the rights and freedoms at issue and, in compliance with the principle of proportionality, must be necessary and genuinely meet the legitimate objective of general interest or the need to protect rights and freedoms of others[127]. In a case regarding an individual who was considered to constitute a terrorist threat, the CJEU held that the competent authorities (i.e., those that requested the measure) must notify him as soon as the notification no longer jeopardizes the investigation, so that the individual can exercise his rights under Articles 7, 8 and 47 of the Charter[128]. In a similar vein, the ECtHR ruled, in a case regarding the use of a surveillance measure, that the notification is to take place once the risk has evaporated[129]. It is unclear when exactly the notification to the target is to take place; there will be the need for clearer criteria to be worked out in the case law, in order to limit the public authorities' discretion.

The abovementioned report by Prof. Fionnuala Ní Aoláin pointed out that victims of unlawful surveillance must have the knowledge and the

December 2015, *Roman Zakharov v. Russia*, Application n° 47143/06, § 230 and 247. See also Article 8 of the Law Enforcement Directive.

122. Judgment of 5 July 2012, *SIAT*, C-318/10, EU:C:2012:415, § 58.

123. Judgments of 10 March 2009, *Hartlauer*, C-169/07, EU:C:2009:141, § 64; of 14 March 2000, *Association Église de Scientologie de Paris*, C-54/99, EU:C:2000:124, § 22; *Commission v. France* ("Elf Aquitaine"), cit., § 50.

124. Indication given by Christoph Brill during the EMFA talk "Safeguarding journalistic sources under Article 4 of the European Media Freedom Act", held on 13 January 2025 at the European University Institute.

125. *Tele 2 Sverige and Watson*, cit., § 121; *La Quadrature du Net 1*, cit., § 190. See also ECtHR, judgments of 4 December 2015, *Roman Zakharov v. Russia*, Application n° 47143/06, § 287; of 28 November 2024, *Klaudia Csikós v. Hungary*, Application n° 31091/16, § 60.

126. See also, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., §§ 117 et seq. regarding the Law Enforcement Directive.

127. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 120 regarding the Law Enforcement Directive.

128. *Ibidem*. For example, to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased and to avail themselves of an effective remedy before a tribunal (*La Quadrature du Net*, § 190).

129. *Roman Zakharov v. Russia*, cit., § 287. See also Voorhoof 2025.

means to use litigation to hold spyware producers to account. Accordingly, not only the existence of the measure, but also the grounds on which the authorization is based, must be notified to the target[130]. National legal rules which exclude, as a general rule, any right to obtain such information are not consistent with EU law[131]. The CJEU ruled that "[t]he right to an effective judicial review, guaranteed by Article 47 of the Charter, requires that the person concerned must be able to ascertain the reasons for a decision taken in relation to him or her, either by reading that decision or by being informed of those reasons, so as to enable him or her to defend his or her rights in the best possible conditions and to decide in full knowledge of the facts whether or not to refer the matter to the court with jurisdiction to review the lawfulness of that decision"[132]. It also held that "once the person concerned has been informed that special investigative methods have been applied to him or her, the obligation to state reasons referred to in the second paragraph of Article 47 of the Charter requires that that person be (…) in a position to understand the reasons why the use of those methods has been authorised, in order to be able, where appropriate, to challenge that authorisation appropriately and effectively"[133].

The judicial or quasi-judicial *ex ante* authorization laid down in Article 4(4)(d) is a guarantee that is essential where the risk of interference with the data subject's rights is serious or even very serious[134]; it plays a very important role in practice, as already mentioned above. Under the ECtHR case law, such authorization must be obtained by the authorities in order to subject the media to secret surveillance measures[135]. The requisite review is to be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not[136]. The court or independent administrative body entrusted with carrying out the prior review must have the power to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation and, on the other hand, the fundamental rights of the persons concerned[137]. If that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence; accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, so that the former is able to carry out the review objectively and impartially and free from any external influence; in particular, in the criminal field, the requirement of independence entails that the body entrusted with the prior review, first, is not to be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-à-vis the parties to the criminal proceedings[138].

The rule of *ex ante* authorization is very important also because it "europeanizes" and "proceduralizes" the issues, by enabling (if it is a court of last instance, by obliging) the judicial organ to make a reference to the CJEU, which constitutes an additional procedural safeguard. The rule of *ex ante* authorization, however, has a limit: in

130. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 120 regarding the Law Enforcement Directive.
131. *Ivi*, § 121.
132. Judgment of 16 February 2023, *HYA*, C-349/21, EU:C:2023:102, § 46.
133. *Ivi*, § 55.
134. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 102 regarding the Law Enforcement Directive.
135. ECtHR, judgment of 22 November 2012, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, Application n° 39315/06, § 101.
136. ECtHR, judgment of 30 August 2022, *Sorokin v. Russia*, Application n° 52808/09, § 46.
137. See, by analogy, judgment *La Quadrature du Net II*, cit., § 125 as regards Article 15(1) of Directive 2002/58.
138. *Ivi*, § 126.

justified cases, the review can take place after the deployment of the surveillance measures[139]. But this exception comes with two caveats: i) the authorization must take place within a "short time"[140] and ii) there must be sufficient guarantees that the exception is used sparingly and only in duly justified cases[141]. In a case regarding surveillance on a journalist, the ECtHR importantly held that the review is to be done at the latest before the access and use of the obtained materials by the public authorities[142]. This exception to this *ex ante* authorization has been criticized for being a possible loophole[143]. It is indeed a risky provision, which is to be interpreted very narrowly precisely because otherwise the main rule would be easily and fully frustrated.

As regards the obligation of recurrent review (which is laid down in Art. 4(6) EMFA), it is noteworthy that the ECtHR held that an assessment is to be made at each stage of the process of the necessity and proportionality of the surveillance measures, namely not only at the moment of the assessment for authorising the measure but also during its execution and thereafter[144]. The case law has specified that when performing the assessment, the court or the independent administrative authority must understand the implications of the surveillance technique used, the nature of the intrusive surveillance software including its relevant technical features, and consider whether its deployment can be limited to certain individuals or groups of individuals[145]. Furthermore, the court or the independent administrative authority must have full and unfettered access to all necessary information, including confidential materials, and that the officials involved in interception activities have a duty to disclose to it any material it requires[146].

In its review of the use of intrusive surveillance software, the judicial or quasi-judicial authority must be able to examine all relevant questions of law and fact for carrying out a proper review of the measure[147]. The individual's right to an effective remedy entails the right to inspect and comment on evidence and observations before the court[148]. This right may be limited by an overriding reason of public interest: the competent organ must verify whether the reasons for the non-disclosure are well-founded[149]. In instances where the ECtHR found the non-disclosure to be justified, and therefore the adversarial principle is limited, it must be counterbalanced by procedural safeguards[150], en-

139. *La Quadrature du Net 1*, cit., § 189; see also ECtHR judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 76 and 81.

140. *La Quadrature du Net 1*, cit., § 189; see also ECtHR, *Szabó and Vissy v. Hungary*, cit., §§ 76 and 81.

141. *Roman Zakharov v. Russia*, cit., § 266.

142. ECtHR, judgment of 14 September 2010, *Sanoma Uitgevers B.v the Netherlands*, Application n° 38224/03, § 91; *Big Brothers v. UK*, cit. See also Voorhoof 2021.

143. Kermer 2024, p. 199.

144. ECtHR, judgment of 6 September 1978, *Klass v. Germany*, Application n° 5029/71, § 55.

145. See for example, *Szabó and Vissy v. Hungary*, cit., § 77.

146. *Roman Zakharov v. Russia*, cit., § 281.

147. Judgment of 16 November 2023, *Ligue des droits humains ASBL, BA v. Organe de contrôle de l'information policière*, C333/22, EU:C:2023:874, §§ 67-69; ECtHR, judgments of 11 June 2019, *Ozdil and Others v. the Republic of Moldova*, Application n° 42305/18, § 68; 15 November 1996, *Chahal v. the United Kingdom*, Application n° 22414/93, § 131.

148. Judgments of 2 December 2009, *European Commission v. Ireland and Others*, C-89/08 P, EU:C:2009:742, § 53; of 4 June 2013, *ZZ v. Secretary of State for the Home Department*, case C-300/11, EU:C:2013:363, § 55. ECtHR, judgment of 19 September 2017, *Regner v. the Czech Republic*, Application n° 35289/11, § 146.

149. *ZZ v. Secretary of State for the Home Department*, cit., § 60. ECtHR, judgments of 19 September 2017, *Regner v. the Czech Republic,* Application n° 35289/11, §§ 152 to 153; 16 February 2000, *Jasper v. the United Kingdom*, Application n° 27052/95, § 56.

150. *ZZ v. Secretary of State for the Home Department*, cit., §§ 57 to 65. *Regner v. the Czech Republic*, cit., § 148; of 29 April 2014, *Ternovskis v. Latvia*, Application n° 33637/02, § 67.

suring that the essence of the right to a fair trial is not compromised[151]. Moreover, the right of individuals cannot be completely emptied: they must, at the very least, be given the substance of the grounds upon which the decision to use surveillance is based[152]. It is however, not self-evident how this case law can be put into practice in the case of spyware. Indeed, as illustrated above, secret surveillance is usually not brought to the knowledge of the individual concerned; moreover, the use of spyware barely leaves traces[153]. That makes it very difficult for individuals to take defensive measures in practice.

According to the Venice Commission, "[g]iven the extraordinary intrusiveness of spyware compared to other surveillance approaches, the screening of authorised and unauthorised (or relevant and irrelevant) information may be difficult as a technical matter. The Venice Commission strongly urges States considering the use of spyware to ensure that it has, as a required safeguard, specialised, vetted, professional teams capable of implementing effective information screening as is required with respect to other information-gathering practices. Destruction requirements [related to unlawfully gathered material] should also be in place, backed up by strong, independent and well-resourced external oversight. This external oversight must be robust and functional both in theory and in practice"[154]. Prof. Ní Aoláin considers in her abovementioned report that if there is no audit record of the spyware activity on a device, the use of spyware is incompatible with human rights law. That is an important finding. At the same time, it has a practical limitation with regard to those instances where spyware is used merely to listen in and not to build evidence[155]. Therefore, it is to be asked whether Member States should not set up, in addition to the independent authority/body provided for in Article 4(8) EMFA, an ombudsman-type of organ with unlimited access to the authorities' surveillance activities. Such an organ would play a complementary and decisive control function, so that there would be an effective check on the use of spyware[156], at least *ex post facto*. Where a State has not established a specialised security oversight body, Data protection Authorities (DPAs) may play an important role in the system of oversight of security and intelligence as a whole[157]. Given the quantity of the data accessed, their sensitive nature and the risk of unlawful access, the data obtained through the use of spyware must be retained in the European Union and must be irreversibly destroyed after the end of the authorization period[158].

Since the common constitutional traditions of the Member States are part of EU law, it is worthwhile to mention some of the rules and constitutional rulings issued by national courts of those States and pertaining to spyware. For example, the German Constitutional Court ruled that public authorities have not only a negative but also a positive obligation to protect fundamental rights from Trojan software attacks against individuals[159]. In a similar vein, the French *Conseil constitutionnel* declared two provisions of a reform of procedural criminal law to be contrary to the French Constitution because they provide for the use of spyware in the pursuit of all kinds of general crimes[160]. Moreover, the law and practice of

151. *Regner v. the Czech Republic*, cit., § 148; ECtHR, judgment of 18 January 2022, *Adomaitis v. Lithuania*, Application n° 14833/18, §§ 68 to 74.

152. See, by analogy, *ZZ v. Secretary of State for the Home Department*, cit., § 65; judgment of 22 September 2022, *GM v. Országos Idegenrendézeti Főigazgatóság*, C-159/21, EU:C:2022:708, § 51.

153. European Data Protection Supervisor 2022, p. 4.

154. Venice Commission 2024, § 85.

155. See, to this effect, *ivi*, § 117.

156. The idea has been given to me by Professor Amnon Reichman in a conversation held at the European University Institute in the autumn of 2024. See to this effect also *ivi*, § 117.

157. *Ivi*, § 118. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 123.

158. See, by analogy, *Tele 2 Sverige and Watson*, cit., § 122.

159. See above fn. 117.

160. *Decision of 16 November 2023, n° 2023-855 DC*, § 68.

third countries is relevant, given the transnational nature of spyware: for example, in the USA, the authorities included NSO (the Israel-based producer of the notorious spyware "Pegasus") in its Entity List for acting against US national security and foreign policy interests, effectively banning USA companies from supplying NSO. In parallel, litigation is being pursued by some USA tech giants against NSO in the USA: on 9 January 2023, the USA Supreme Court ruled that WhatsApp (belonging to Meta - former Facebook) is allowed to pursue a lawsuit against NSO with regard to the deployment of Pegasus. On 20 December 2024 a federal USA judge ruled that NSO was liable under USA federal and California law for hacking activity that breached over 1,000 WhatsApp users in 2019[161].

In conclusion, whilst spyware is a matter that presents many technical issues, it is, first and foremost, a question of major constitutional importance, raising issues such as: the competences of the Union to regulate the matter (even going beyond EMFA), the compliance with fundamental rights, and the translation of the values under Article 2 TEU into legislation and enforcement action. In this context, legal tensions often arise such as the tension between the constitutional identity of the Union and the constitutional identity of the Member States (e.g., with regard to national security): the reconciliation between both identities is probably one of the most difficult legal challenges that the Union and its Member States will have to face in the near future. The regulation of spyware is one of the most interesting litmus tests for examining the interplay between these constitutional identities[162]. In this context, it should be recalled that, as explained above, EU law, including the protection of fundamental rights (also in light of the ECHR) remains applicable also when national security is invoked.

3. The issue of legal basis: media-specificities and misunderstandings?

This leads to the issue of the legal basis for Article 4 EMFA and for the Act in general. The EMFA is based on Article 114 TFEU, which is the general internal market legal basis in the EU treaties. During the first part of the negotiation process, the issue of the legal basis of EMFA was hotly debated. Political and private entities and Member States which perceived the EMFA as an intolerable intrusion into their political or business autonomy rallied against the legal basis. The ensuing discussion was intense and not always deprived of ideology. Ideally, the debate, in order to be objective, would have relied on a complete picture of the CJEU case law regarding Article 114 TFEU as legal basis and would have engaged with the details of the Commission's impact assessment and with the content of the Commission's proposal for EMFA. It is an open question whether that has always been the case. In any event, a turning point in the debate was the issuance on 4 April 2023 of the Opinion by the Council Legal Service confirming in substance that Article 114 TFEU can be used as legal basis of the EMFA[163].

In the debate, one of the criticisms against the legal basis of the EMFA is that it regulates the cultural and fundamental rights aspects of the media[164]. This criticism, even when expressed in good faith, relies on a misconception both of what internal market legislation does and of the characteristics of the media sector. The Treaty, by establishing a common market and progressively approximating the economic policies of the Member States, seeks to unite national markets into a single market having the characteristics of a domestic market[165]. When regulating the internal market, the legislator pursues the cross-national integration of markets and their "opening up", and at the same time – precisely because it creates new freedom spaces on the market – it also needs to

161. Lyngaas 2024.

162. The idea has been given to me by Alberto De Gregorio Merino in a conversation in the 2023/24 winter at the Legal Service of the European Commission.

163. Opinion 8089/23.

164. See also Cornils 2024 under I, 2. and III.

165. Judgment of 9 February 1982, *Polydor*, Case 270/80, EU:C:1982:43, § 16.

take care of overriding reasons of public interest[166]. To that end, the legislator may, and in fact, must take into account the EU's values and fundamental rights[167]. Even though Article 2 TEU (laying down the values of the EU) and the Charter of fundamental rights of the EU do not establish competences in themselves, they set up requirements for legislation[168]. As the Council Legal Service in its Opinion on the legal basis of EMFA observed, "pluralism is recognised as an essential attribute of society in Article 2 TEU, which sets out the values on which the Union is founded. The Court has ruled on 16 February 2022 on the rule of law conditionality regulation that 'the European Union must be able to defend those values, within the limits of its powers as laid down by the Treaties'. This case law indicates that the Union legislature is empowered to ensure the protection of the values mentioned in Article 2 TEU and of other fundamental rights where it has an appropriate legal basis for taking legislative action"[169].

So, for example, when harmonizing the production and sale of mundane products such as heating system devices in the EU, the legislator not only harmonizes the rules by integrating and opening up the market, but also by taking care of further public interests such as the safety of users, environmental protection, the protection of consumers, and the protection of privacy. This holistic nature of the legislator's action is, as such, neither unlawful nor extraordinary[170]: not unlawful because the legislator is bound to further the values of the EU when disbursing its task, and not extraordinary because socio-economic phenomena cannot be split into purely economic aspects, on the one hand, and other aspects on the other[171]. Such splitting would be artificial and would not reflect the multifacetedness and complexity of reality. This is particularly true for the media, which differs from other products such as heating system devices. Since media are "special goods" and media freedom represents not only a feature of the media service, but also a cornerstone of democracy shaping public opinion and the consequent political decisions, the malfunctioning of the media market might go hand in hand with breaches to the rule of law[172].

What is crucial for the purposes of the legal basis analysis of the EMFA is that the freedom and independence of the media are not only comprised by the fundamental rights protection but also contribute to the quality of the service: as noted above, a media service produced without full editorial freedom and independence lacks quality and thus this aspect is important for the good functioning of the internal market, as it follows from recitals 16 and 17 EMFA. Therefore, economic aspects are not a mere pretense to regulate fundamental rights in the EMFA. The fact that a media service provider is – directly or indirectly, actually or potentially – interfered with in the exercise of its economic activity entails a restriction of its economic rights in the internal market and an uneven playing field. That in turn has repercussions on editorial freedom and independence.

Those who overlook that circumstance fall into the second misconception. Indeed, in order to provide a basis for mutual recognition in the internal market, traded products must fulfill certain basic production standards, such as food safety regulations, as well as other requirements for the protection of consumers[173]. The same applies to media services: as explained, editorial independence and freedom constitute basic quality standards for the media services. Therefore, the regulation of the economic aspects of media necessarily entails at least some regulation of the related fundamen-

166. See, *ex multis,* Judgment of 3 December 2019, *Czech Republic v. European Parliament and Council*, C-482/17, EU:C:2019:1035, § 36.

167. Judgment of 22 January 2013, *Sky Österreich*, C-283/11, EU:C:2013:28, § 51.

168. Judgment of 29 July 2024, *Valančius*, C-119/23, EU:C:2024:653, § 47. See also Bayer 2024, p. 116; Longo 2025, pp. 9-10.

169. Opinion 8089/23, § 55.

170. See also Roß 2023, p. 460.

171. See also Malferrari 2023, pp. 49-50.

172. Brogi–Da Costa Leite Borges–Carlini et al. 2023, p. 38.

173. Bayer 2024, pp. 114-115; Malferrari–Gerhold 2024, pp. 894-895.

tal right aspects, because in the case of the media, they are inextricably intertwined with each other and represent two sides of the same coin[174]. In other words, the value-laden nature of the media sector[175] obliged the legislator to properly take the values and fundamental rights into account when regulating the media services. Indeed, the media market is the marketplace of ideas and opinions, so that regulating that marketplace entails taking into account the freedom of expression and the cultural characteristics of the media. As explained in the Explanatory memorandum accompanying the Commission proposal[176], "[t]he EU legislator must not only comply with fundamental rights when regulating the internal market, but also balance competing fundamental rights. The present Regulation proposal constitutes a harmonious, coordinated and multi-pronged legislative framework by which the legislator contributes to the development and protection of the internal market for media services, thereby also pursuing several further legitimate public interests (including the protection of users) and reconciling in a fair manner the fundamental rights of all the individuals concerned". The Council Legal Service, in its Opinion on the legal basis of EMFA, remarked that "ensuring the quality of media services or protecting media freedom does not as such exclude the use of Article 114 TFEU"; it further explained as follows: "[e]ven though Article 114(3) TFEU does not mention the freedom and pluralism of media – unlike for example a high level of health protection, environmental protection or consumer protection – it is inherent in the harmonisation under Article 114 TFEU that national rules are harmonised which are taken in the pursuit of specific policies. It is therefore inherent in the logic of Article 114 TFEU that the Union rules harmonising these national rules will relate to these policies. Protecting the freedom of the media and the quality of media services can thus be an essential public interest objective in a legislative act based on Article 114 TFEU if the conditions set out therein are fulfilled"[177]. In light of the foregoing, the legislator in the EMFA cannot be validly criticized for having taken into account the cultural diversity and pluralism of the media when regulating the media services market.

That does, of course, not mean that the conditions for using Article 114 TFEU as the legal basis can be neglected: such conditions must be verified (see more in detail below). But it means that the EMFA cannot be validly criticized for having prominently taken the values fundamental rights into account when regulating the media services: an impact on them is inherent in the nature of the media services. By the same token, an indirect impact on the cultural aspects of the media services cannot be avoided in the case of EMFA precisely because media services have an inherent cultural dimension. Such an impact is, as such, not unlawful and is even implied by Article 167 TFEU, whereby the legislator is to take account of the cultural aspects when using legal bases provided for in the Treaties (such as Article 114 TFEU).

Having made these clarifications, I now examine whether the conditions for using Article 114 TFEU are fulfilled in the case of the EMFA. Since the present essay is concentrated on Article 4 EMFA, I will limit the analysis to that provision. As is well known, Article 114 TFEU, in essence, requires that: i) there is actual or likely regulatory fragmentation; ii) the fragmentation leads to restrictions to the fundamental freedoms or to an uneven playing field, to the detriment of the good functioning of the internal market, iii) the internal market problem is solved through the envisaged EU harmonization[178].

In the case of Article 4 EMFA, first, the State's interferences in or influencing of the editorial policies and editorial decisions of media service

174. Roß 2023, p. 459. See also, to this effect, Vīķe-Freiberga–Däubler-Gmelin–Hammersley–Poiares Pessoa Maduro 2013, p. 20.

175. Council conclusions on safeguarding a free and pluralistic media system (2020), § 18.

176. COM(2022) 457, p. 8.

177. Opinion 8089/23, § 54. See, to this effect, *Sky Österreich*, cit., § 52, and judgment of 3 February 2021, *Fussl*, C-555/19, EU:C:2021:89, §§ 54-55 and case law cited therein. See also Vidal Marti 2023.

178. See, *ex multis,* Judgment of 12 December 2006, *Germany v. European Parliament and Council* (Tobacco Advertising II), C-380/03, EU:C:2006:772, §§ 36 et seq.

providers constitute restrictions to the free exercise of the media service activities in the internal market because the quality of media services requires freedom in the making of the media products: like an industrial product requires the respect for safety standards and a medical service requires the autonomy of diagnosis by the medical professionals, the media service requires the autonomy of the media service providers from the State. Since the media services are increasingly liable to be produced or consumed cross-border[179], a cross-border element is typically present at least in many scenarios[180]. In that regard, recourse to the legal basis of Article 114 TFEU does not presuppose the existence of an actual link with freedom of movement between Member States in each of the situations referred to by the act founded on such a basis. What is important, in order to justify recourse to that legal basis, is that the act adopted on that basis actually has as its object the improvement of the conditions for the establishment and functioning of the internal market. As regards journalistic sources and confidential information related to or capable of identifying journalistic sources, they constitute the "raw material" of the media services, so that their disclosure entails losing their economic value and function for the media service providers, to the detriment of the exercise of the media service activities (see recital 19 EMFA). The same reasoning applies to the detainment, sanctioning, interception and inspections of media service providers or their editorial staff: if the service provider is impaired in its function, a restriction to the exercise of its economic activity is present. The same goes for the deployment of spyware.

Second, the rules protecting editorial independence and journalistic sources are heterogenous across the internal market (recitals 18 and 23 EMFA and Commission's Impact Assessment, pages 8-9)[181]. In particular, in some countries, the data protected by the secrecy of a journalistic sources cannot be collected or analyzed, whereas in other countries, the limits are very different[182]. This finding has been reaffirmed by the Venice Commission as regards spyware[183]. Furthermore, the application of the divergent rules gives rise to legal uncertainty, to the detriment of the good functioning of the internal market[184]. As stated in recital 24 EMFA, "(m)edia professionals, in particular journalists and other media professionals involved in editorial activities, work increasingly on cross-border projects and provide their services to cross-border audiences and, by extension, to media service providers. As a result, media service providers are likely to face barriers, legal uncertainty and uneven conditions of competition. Therefore, the protection of journalistic sources and confidential communications requires harmonisation and further strengthening at Union level". This internal market problem for media service providers is solved by Article 4 EMFA because it opens up the market and lays down a common (minimum) protection for media service providers. It cannot, thus, be validly argued that the EMFA merely has positive side effects for the internal market[185].

It follows from the foregoing considerations that the requirements for the use of Article 114 are fulfilled as regards Article 4 EMFA.

The fact that the legislator limited itself to principled rules and to minimum protection testifies to the respect for subsidiarity and proportionality. In particular, the subsidiarity condition is fulfilled because in the Member States, political forces were

179. Longo 2025, p. 9.

180. See, to that effect, judgments of 20 May 2003, *Österreichischer Rundfunk*, C-465/00, EU:C:2003:294, § 41; of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, § 40.

181. Parcu–Brogi–Verza et al. 2022, pp. IV, 188, 326-327, 351, 366.

182. Venice Commission 2024, § 42.

183. *Ivi*, §§ 37 et seq. (see in particular 61).

184. Cf. *ivi*, § 82: "[w]hile some domestic legal regimes are quite detailed and precise, some others tend to rely on relatively broad and open-ended formulations which do not necessarily provide the required degree of certainty and precision".

185. See, to that effect, Longo 2025, p. 10; Mastroianni 2022, p. 107. But for a different view see Kraetzig 2023, p. 1; Cornils 2024, under III. 3. a).

unwilling to modify the regulatory framework that facilitated or created the market failures that affect the European media market[186]. The choice of a regulation instead of a directive is justified when considering the need for rapid regulation of the digital market[187].

A criticism raised against Article 114 TFEU as the legal basis for Article 4 EMFA is that it violates the Member States' competence for criminal law[188]. This criticism is unfounded. Indeed, Article 4 TFEU does not directly harmonize national criminal law: see also recital 22 EMFA, *in fine*, whereby "[i]t is not the purpose of this Regulation to harmonise the concepts of 'detain', 'inspect', 'search and seizure' or 'surveillance'". Article 4 EMFA rather creates a frame ("encadrement") within which Member States must exercise their competences, be they of an administrative, criminal or private law nature (provided of course that the limits set by Article 114 TFEU are complied with). In that regard, Article 4 EMFA is similar to the Directive on personal data, the e-privacy Directive, and the Regulation on the free flow of non-personal data, which are also based on Article 114 TFEU[189]. The Union's competence to harmonize national law pursuant to Article 114 TFEU is a functional competence; it is not thematically limited, and applies to any measure that affects the establishment or functioning of the internal market[190].

In conclusion, given its novelty, it is understandable that the EMFA raises an issue of legal basis. However, in light of the well-established case law of the CJEU, the examination of the articles of the EMFA, its recitals, the Explanatory Memorandum and the Impact Assessment of the Commission offer more than a sufficient and solid ground for considering Article 114 TFEU as a lawful legal basis. That issue will be adjudicated by the CJEU because Hungary has lodged an annulment action against EMFA as regards the legal basis; the case is pending at the time of writing[191].

4. The future prospects of enforcement of Article 4 EMFA

Article 4(1) and (2) EMFA are applicable since 8 February 2025, whereas the rest of Article 4 EMFA will be applicable from 8 August 2025[192]. A number of issues related to the application of Article 4 EMFA are to be considered at this stage. First, how can it be ensured that the guarantees laid down in Article 4(4) and (5) EMFA are rendered effective in practice? The secrecy of surveillance measures is to be respected (at least to a certain extent) so that at least in many cases, both the authorization of surveillance measures and their execution are carried out without the individual's knowledge. On the other hand, the *effet utile* of Article 4 EMFA requires that measures are taken such as to avoid the guarantees becoming nugatory. In this regard, Article 4(8) EMFA, in its second part, is pertinent. Under this provision, Member States shall entrust an independent authority or body with relevant expertise to provide assistance, with regard to the exercise of the right to effective judicial protection, to media service providers, their editorial staff and any persons who, because of their regular or professional relationship with a media service provider or its editorial staff, might have information related to or capable of identifying journalistic sources or confidential communications. Candidates for being the independent authority or body referred to in this provision could be the data protection

186. Bayer 2024, p. 113.

187. Longo 2025, p. 9.

188. Cf. Ferreau 2024, p. 43.

189. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

190. Schütze 2014, a p. 228.

191. *Hungary v. European Parliament and Council*, C-486/24.

192. Article 29 EMFA.

representative, but it could also be an *ad hoc* authority or even a private entity such as a media service provider chamber or journalist association. An important role to be played by this independent authority or body is to supervise the authorization and the execution of surveillance measures (including verifying the duration and ensuring that the conditions are still being met). The need for the abovementioned independent authority or body is indirectly underpinned by the Venice Commission, which recognized that the absence of information for the target of surveillance measures can, to some extent, be compensated by the presence, in the procedure, of bodies acting as "privacy advocates", i.e., legal professionals that represent the interests of targeted persons and organizations in the authorization procedure[193].

Strict confidentiality obligations can be imposed on the privacy advocates. A security screened advocate does not directly act for the suspect and cannot, obviously, consult with him or her. The advocate may, in practice, be given only a very short time to familiarize with the particulars of the case, and thus be at a procedural disadvantage compared to the requesting authority; on the other hand, the mechanism can still have some value insofar as it can lead to conditions being imposed to minimize the intrusion into privacy, either for the target, or others affected by the surveillance[194]. Moreover, it can formalize the process of obtaining authorization, making it clearer that it is the requesting authority which has the burden of showing the need for the use of surveillance, and that all the conditions for surveillance need to be fulfilled[195].

Second, the media service provider target of surveillance still needs to be notified *ex post facto*, so that he/she can exercise his/her right to judicial remedies, including review and damages actions. During the exercise of that right, there are practical issues that are thorny: are there limits to the scope of the judicial review that arise from the confidentiality of national or public security reasons? It is conceivable that certain documents must be redacted or made entirely confidential; this, however, does not rule out the effective review by a judge, who can handle confidentially reports or other documents (in their entirety or partially redacted). Furthermore, there are doubts about the adequacy of the safeguards where the applicant's presumed situation is such that the information on the authorization of covert information gathering remains confidential and therefore inaccessible to the person concerned[196]. There are some, at least, partial solutions that can be envisaged. For example, a complaint mechanism can be set up to make the review effective; access to classified information can be given to remedial bodies[197]. Furthermore, the use of in-camera proceedings may also provide a practical solution. In addition, the independent authority or body referred to in Article 4(8) EMFA could also be given access to confidential information, on the basis of which it could react in the interest of the individual concerned. According to settled case-law, "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law; thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[198].

A third issue regarding the application of the provision is whether a judge who has to decide on the prior authorization under Article 4(4)(d) EMFA may pose a preliminary question to the CJEU. As is well-known, one of the conditions for the admissibility of a preliminary reference is that a legal dispute is pending before the referring

193. Venice Commission 2024, § 113.

194. *Ibidem*.

195. *Ibidem*.

196. *Klaudia Csikós v. Hungary*, cit., § 66.

197. European Union Agency for Fundamental Rights 2023; Venice Commission 2024, § 123.

198. Judgment of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, § 187.

judge[199]. In the present scenario, there is, at least nominally, a counterpart which is the person who is to be subjected to surveillance ("the target"). The fact that this person is excluded from the procedure on the ground of the confidentiality of the investigation does not make the adversarial nature of the procedure evaporate. There is, on the merits of the case, a dispute before the authorizing judge, who would thus be empowered to refer a question of interpretation and/or validity to the CJEU under Article 267 TFEU[200]. The reference however should be drafted in such a way that several details are made confidential, in order to avoid the risk that the individual recognizes his/her situation and thus becomes aware in advance of the fact of being subject or being liable to be subject to surveillance.

A fourth issue concerns the role to be played by the media regulators and the Board (which consists of the national regulators pursuant to Article 10(1) EMFA). In the first place, the Board, upon the Commission's request, is to draft opinions on technical and factual issues related to Art. 4(4)(c)[201]. The Board's decisions are taken with a 2/3 majority. Whereas these opinions are by definition not binding, they carry some weight in the assessment to be made by national authorities, which must take them into account on the ground of loyal cooperation under Article 4(3) TEU. According to recital 41, the Board's opinions "should serve as useful guidance for the national regulatory authorities or bodies concerned and could be taken into account by the Commission in its tasks of ensuring the consistent and effective application of this Regulation and the implementation of Directive 2010/13/EU. By making their best effort to implement the opinion of the Board or by properly explaining any deviation therefrom, national regulatory authorities or bodies should be considered to have done their utmost to take the opinion of the Board into account". In the second place, the Board shall, inter alia, "promote cooperation and the effective exchange of information, experience and best practices between the national regulatory authorities or bodies on the application of (…) this regulation"[202]. The Board shall foster the exchange of best practices among the national regulatory authorities or bodies, consulting stakeholders where appropriate, on regulatory, technical or practical aspects relevant to the consistent and effective application of this Chapter of the EMFA and the implementation of AVMSD[203].

A fifth and final issue concerns the role to be played by professional associations, in particular journalist associations. Their role is not prominently provided for in EMFA. There is reference to "other relevant bodies and sources" made in Article 27(4)(a) EMFA in the context of the evaluation and reporting to be carried out by 8 August 2028. According to recital 40, "[w]here the Board deals with matters beyond the audiovisual media sector, it should rely on an effective consultation mechanism involving stakeholders from the relevant media sectors active both at Union and national level. Such stakeholders could include press councils, journalistic associations, trade unions and business associations. The Board should give such stakeholders the possibility to draw its attention to the developments and issues relevant to their sectors. The consultation mechanism should enable the Board to gather targeted input from the relevant stakeholders and obtain relevant information supporting its work. When establishing the arrangements for the consultation mechanism in its rules of procedure, the Board should take into account the need for transparency, diversity and fair geographical representation. The Board should also be able to consult academia in order to gather additional relevant information". Going beyond this, professional associations may play a decisive role in providing input to further institutional actors, in bringing collective actions via national

199. See, *ex multis,* Order of 18 June 1980, *Borker*, Case 138/80, EU:C:1980:162, § 4.

200. See, to this effect, *Procura di Bolzano*, cit., which concerned the request for authorisation from a judge in order to access personal data retained by providers of electronic communications services, with a view to the prosecution of crimes.

201. Article 13(1)(c)) EMFA.

202. Article 13(1)(b) EMFA.

203. Article 16(1) EMFA.

procedural law channels and in assisting media service providers on legal and technical matters.

5. Conclusion

The internal market cannot be confined to a purely welfare-maximizing project. Whereas the values enshrined in Article 2 TEU are formulated in broad terms, they have a legal significance that must be preserved and propagated (cf. Article 3 TEU)[204]. Public powers in the EU are bound to pursue the values shared by the EU and its Member States. A common EU media policy that would better concretize the European values is an indispensable precondition for the European integration project especially considering the deepening of the geopolitical crisis[205]. Indeed, the media have been under attack in the Union in several ways. Political forces and national governments often perceive free media as a nuisance at best and otherwise as a tool to be domesticated and used for their purposes; in the worst case, free media are even considered to be a hindrance that must be gotten rid of. Furthermore, social media and non-journalistic content have been increasingly consumed by citizens and undertakings in lieu of proper media services[206]. Truth is a rare and expensive commodity[207]. Disinformation and AI-produced content are certainly cheaper to produce and easier to get the favor of algorithms, which aim at maximizing users' engagement and thus gives disproportionate resonance to polarizing or radical content. Thus, quality media services risk remaining squeezed in the digital and AI era. In addition, risks to the EU's internal media market from third countries are increasing: for ex., foreign misinformation is systematically used as a "weapon"[208].

Against this dire backdrop, the need for a liberal legal protection of the media services at European level can barely be called into question. Since for the media the challenges related to the market and the values are increasingly cross-border and the hindrances stem from national actors (mainly governmental ones), it was for the EU to step in and act. Obviously, the EMFA is not a panacea for the many arduous challenges affecting the media services in the internal market. But, albeit minimalist, the EMFA tries to address these challenges. In particular, it safeguards the rights of media service providers, including journalists, and protects their independence in many regards; by doing so, the EMFA not only develops the internal market further, but it also paves the way for a more resilient and democratic European Union[209]. The obligation of effective editorial freedom and independence of media service providers and the prohibition to interfere in or try to influence their editorial policies and editorial decisions give more precision to existing obligations under the Charter and the ECHR. The relevance of Art. 4 (3-9) EMFA consists in particular in creating a supranational level of normativity and an additional layer of control of implementation which is important because there is limited compliance in several Member States with the ECtHR's case law on Article 10 ECHR. The tandem of the national judiciary as *juge commun du droit européen* and the CJEU as well as the Commission through the infringement procedure offer enforcement possibilities which the ECHR does not possess.

The internal market is a living instrument[210]. The EMFA can be considered to be an impressive example of the vitality and dynamism of the Union legislation as instrument of policy making[211]. The EMFA develops the internal market law in light of the fundamental rights laid down in the Charter of fundamental Rights, by strengthening existing guarantees and enabling a vibrant economic sector to regain thrust and to develop further, including

204. See AG Ćapeta Opinion in *Commission v Hungary* ("anti-LGBTQ"), C-769/22, EU:C:2025:408, § 155 et seq.

205. Bayer 2024, p. 109.

206. Newman 2024.

207. Harari 2024, p. 17.

208. Article 17 EMFA aims at tackling this problem in particular. See Malferrari 2023, pp. 49-50.

209. Verheyen 2024.

210. See, to this effect, Opinion of AG M. Szpunar of 18 May 2017, *Visser*, Joined Cases C-360/15 and C-31/16, EU:C:2017:397, § 2.

211. Cf. Cornils 2024, VI.

across borders[212]. The economic aspect of the media and their value-laden nature constitute two sides of the same coin they are merged with each other in the EMFA. There is harmony between the EU's economic efficiency (in particular through the opening of the markets and free competition) and its values, because the reconciliation of all those public objectives is the cement that keeps individuals and society together in a regionally, culturally and socially diverse and sometimes divergent Europe[213]. Thus, the EMFA also contributes to the development of a European society, which is an immensely valuable resource for current and future generations.

References

J. Bayer (2024), *Digital Media Regulation within the European Union. A Framework for a New Media Order*, Nomos, 2024

E. Brogi, D. Da Costa Leite Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, Study PE 747.930, 2023

M. Cole, C. Etteldorf (2024), *The European Media Freedom Act unpacked*, European Audiovisual Observatory, 2024

M. Cole, C. Etteldorf (2023), *European Media Freedom Act – Background Analysis*, European Parliament Policy Department for Structural and Cohesion Policies, Directorate-General for Internal Policies, PE 733.129, 2023

M. Cornils (2024), *Der Funktionsschutz der Medien als Aufgabe des Unionsrechts*, in "Zeitschrift für Gesetzgebung", vol. 39, 2024, n. 4

European Union Agency for Fundamental Rights (2023), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU*, 2023

European Court of Human Rights (2022), *Guide on Article 10 of the European Convention on Human Rights – Freedom of expression*, 2022

European Data Protection Supervisor (2022), *Preliminary Remarks on Modern Spyware*, 15 February 2022

J.F. Ferreau (2024), *Rechte von Mediendienstanbietern (Art. 4)*, in Id. (ed.), "Das neue EU-Medienfreiheitsgesetz", Nomos, 2024

L. Gerhardinger (2023), *Journalistischer Quellenschutz im Zeitalter der Digitalisierung und Globalisierung*, Mohr Siebeck, 2023

O. Grandinetti (2024), *Quale nozione di pluralismo nell'EMFA?*, in "Rivista italiana di informatica e diritto", 2024, n. 2

Y.N. Harari (2024), *Nexus. A Brief History of Information Networks from the Stone Age to AI,* Random House, 2024

K. Jakubowicz (2015), *New Media Ecology: Reconceptualizing Media Pluralism*, in P. Valcke, M. Süksöd, R.G. Picard (eds.), "Media Pluralism and Diversity", Palgrave Macmillan, 2015

J.E. Kermer (2024), *Article 4 of the European Media Freedom Act: A Missed Opportunity? Assessing Its Shortcomings in Protecting Journalistic Sources*, in K. Simeonov, M. Yurukova (eds.), "The Agenda of

212. See also Paolucci 2024.

213. See Triantafyllou–Malferrari 2022, p. 330. Cf. also von Bogdandy 2024, pp. 11-13.

the New EU Institutional Cycle. Papers from the Eleventh International Scientific Conference of the European Studies Department", Sofia University, 2024

J.E. Kermer (2024-a), *How far does Article 4 of the European Media Freedom Act go in banning state surveillance of journalists?*, Centre for Media Pluralism and Media Freedom, 26 November 2024

V. Kraetzig (2023), *Freedom Governed by Brussels*, in "Verfassungsblog: On Matters Constitutional", 12 June 2023

E. Longo (2025), *Grounding media freedom in the EU: The legal basis of the EMFA*, in "Rivista italiana di informatica e diritto", 2025, n. 1

S. Lyngaas (2024), *Judge rules Israeli firm NSO Group liable for damages in WhatsApp hacking case*, CNN, 20 December 2024

L. Malferrari (2023), *Der European Media Freedom Act als intra-vires-Rechtsakt*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 34, 2023, n. 49

L. Malferrari, M. Gerhold (2024), *Ein Unionsrecht auf Empfang pluraler Medien?*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 35, 2024, n. 19

R. Mastroianni (2022), *Freedom and pluralism of the media: an European value waiting to be discovered?*, in "MediaLaws", 2022, n. 1

H. Mildebrath (2022), *Europe's PegasusGate. Countering spyware abuse*, European Parliamentary Research Service, 2022

N. Newman (2024), *What do we Know about the Rise of Alternative Voices and News Influencers in Social and Video Networks?*, Digital News Report 2024 sec. 2.5, Reuters Institute and University of Oxford, 2024

F. Ní Aoláin (2023), *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism – Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, UN Human Rights Council, 2023

F. Palmiotto (2024), *Criminal investigations, access to data and fundamental rights: The role of judicial review after Procura*, in "Common Market Law Review", vol. 61, 2024, n. 6

F. Paolucci (2024), *The European Media Freedom Act: (another) new chapter in the digital regulation saga*, in "Diritti Comparati", 6 May 2024

P.L. Parcu, E. Brogi, S. Verza et al. (2022), *Study on media plurality and diversity online*, Publications Office of the European Union, 2022

R. Phillips (2023), *The Efficacy of European Union Spyware Regulations*, in "Student Occasional Paper", Tech4Humanity Lab, 2023, n. 5

H. Raab (2022), *Wie wir die Freiheit der Medien bewahren*, in "Frankfurter Allgemeine Zeitung", 30 July 2022

Reuters (2025), *Italian government under pressure in Paragon spyware row*, 7 February 2025

Reuters (2024), *Digital News Report 2024*

L. Roß (2023), *European Media Freedom Act und Kernfragen der europäischen Integration*, in "Europarecht", vol. 58, 2023, n. 5

R. Schütze (2014), *Limits to the Union's 'Internal Market' Competence(s): Constitutional Comparisons*, in L. Azoulai (ed.), "The Question of competence in the European Union", Oxford University Press, 2014

M. Trevisan, V. Štětka, M. Milosavljevič (2024), *Tools and strategies of political capture of the media in Europe*, in E. Brogi, I. Nenadić, P.L. Parcu (eds.), "Media Pluralism in the Digital Era", Routledge, 2024

D. Triantafyllou, L. Malferrari (2022), *The European Commission: the clock master of the European Union Internal Market*, in European Commission (ed.), "70 Years of EU law – A Union for its citizens", Publications Office of the European Union, 2022

P. Valcke, R.G. Picard, C. Dal Zotto (2015), *Indicators for Media Pluralism*, in P. Valcke, M. Süksöd, R.G. Picard (eds.), "Media Pluralism and Diversity", Palgrave Macmillan, 2015

Venice Commission (2024), *Report on a rule of law and human rights compliant regulation of spyware*, CDL-AD(2024)043, 13 December 2024

S. Verheyen (2024), *Der Europäische Medienfreiheitsakt: Ein Meilenstein für die Pressefreiheit in der EU*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 35, 2024, n. 12

S. Verza (2025), *What is journalism in the digital age? Key definitions in the European Media Freedom Act*, in "Rivista Italiana di informatica e diritto", 2025, n. 1

N. Vidal Marti (2023), *The Key to Ensure Media Pluralism in the EU? A Unified Framework*, in "Verfassungsblog: On Matters Constitutional", 12 June 2023

V. Vīķe-Freiberga, H. Däubler-Gmelin, B. Hammersley, L.M. Poiares Pessoa Maduro (2013), *A free and pluralistic media to sustain European democracy*, European Commission, 2013

A. von Bogdandy (2024), *On the Meaning and Promise of European Society*, in "MPIL Research Paper Series n. 2024-30", 2024

D. Voorhoof (2025), *European Court of Human Rights: Klaudia Csikós v. Hungary*, European Audiovisual Observatory, 2025

D. Voorhoof (2022), *European Media Freedom Act and the protection of journalistic sources: still some way to go*, 18 November 2022

D. Voorhoof (2021), *Case Law, Strasbourg: Big Brother Watch v. United Kingdom, Bulk interception regime violated Articles 8 and 10*, 9 June 2021

S. Woodhams (2021), *Spyware: An unregulated and Escalating Threat to Independent Media*, Centre for International Media Assistance (CIMA), 25 August 2021

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0227 • articolo sottoposto a peer review • pubblicato in anteprima il 1 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Jan Erik Kermer

The delicate balancing between media pluralism and market freedom: Analysing the procedural safeguards for the media under Article 21 of the EMFA

Article 21 of the European Media Freedom Act aims to ensure that Member State measures potentially affecting media pluralism or EU market freedoms must be justified, proportionate and meet several procedural requirements. Article 21 lays the groundwork for the media plurality test, in Article 22 by regulating, inter-alia, limits on cross-sector media ownership to prevent market failures and protect media pluralism. This article is timely, enabling the media to appeal against state measures considered harmful to the freedom of establishment and media pluralism, which have become integral to the EU's normative identity. Years before the EMFA was conceived, these freedoms culminated in a protracted legal dispute between Vivendi SA and Mediaset. This case served as an important catalyst for the revision of Italy's anti-trust law and Article 21 of the EMFA, thereafter. This paper summarises how this landmark case unfolded while highlighting its parallels with Article 21 of the EMFA. Thereupon, it summarises the debate concerning the contestable legal basis of this article. The paper concludes by elucidating the provision's potential shortcomings, which may pose legal certainty and enforcement issues.

European Media Freedom Act, Article 21 – Media pluralism – Media ownership

Il delicato equilibrio tra pluralismo dei media e libertà di mercato: un'analisi delle tutele procedurali per i media ai sensi dell'articolo 21 dell'EMFA

L'articolo 21 dell'European Media Freedom Act mira a garantire che le misure degli Stati membri potenzialmente incidenti sulla pluralità dei media o le libertà di mercato dell'Unione europea siano giustificate, proporzionate e rispettino diversi requisiti procedurali. L'articolo 21 pone le basi per il test della pluralità dei media, specificato all'articolo 22, regolando la limitazione della proprietà dei media da parte di altri settori al fine di prevenire i fallimenti del mercato e salvaguardare il pluralismo dei media. Questo articolo è una disposizione tempestiva, in quanto i fornitori di servizi mediatici hanno ora il diritto di presentare ricorso contro le misure statali considerate minacciose per la libertà di stabilimento e il pluralismo dei media, che sono diventati parte integrante dell'identità normativa dell'Unione Europea. Anni prima della concezione dell'EMFA, queste libertà sono culminate in una lunga disputa legale tra Vivendi SA e Mediaset. Questo caso ha rappresentato un importante catalizzatore per la successiva revisione della legge antitrust italiana e dell'articolo 21 dell'EMFA. Il presente manoscritto riassume l'evoluzione di questo caso emblematico, evidenziandone i parallelismi con l'articolo 21 dell'EMFA. In seguito, fornisce una sintesi del dibattito sulle controverse basi giuridiche di questo articolo. Questo contributo si conclude illustrando le potenziali carenze della disposizione, le quali potrebbero porre problemi di certezza del diritto e di applicazione.

European Media Freedom Act, Articolo 21– Pluralismo dei media– Proprietà dei media

The Author is Research Associate at the Centre for Media Pluralism and Media Freedom, European University Institute

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: Introduction. – 1. Vivendi vs Mediaset: An important precursor to Article 21. – 2. An overview of Article 21's main provisions. – 3. Assessing the legal basis of Article 21. – 4. A critical examination of Article 21. – 5. Conclusion: A counterfactual highlighting the added value of Article 21 EMFA.

Introduction

Four freedoms – namely, goods, services, people and capital – underpin the functioning of the European Union's internal market. These freedoms, however, are not inviolable, as Article 49 of the Treaty on the Functioning of the European Union (TFEU) has established, and numerous cases of the Court of Justice of the European Union (CJEU) case law have clarified. This is the underlying logic of Article 21, which sets forth the principle that media service providers (MSPs) should be able to carry out their services without interference in the internal market (see also Art. 4(1) EMFA). This economic freedom may, however, be justifiably restricted if the editorial independence of an MSP is 'likely' to be negatively impacted. Article 21 of the European Media Freedom Act (EMFA) introduces rules aimed at safeguarding media pluralism – which has become a central pillar of the normative fabric of the EU (see, for instance, Art. 11 CFR) – as well as reinforcing the freedom of establishment (Art. 49 TFEU). Article 21 of the EMFA, in essence, aims to regulate the ostensible tension between these market and non-market freedoms. Striking a balance between them has proven difficult in the past, as elucidated by the protracted legal dispute between Vivendi and Mediaset (a detailed analysis of this case is presented below). Article 21 lays the groundwork for Article 22's so-called "media plurality test" by regulating, inter-alia, the limiting of media ownership by other sectors (as stated in Recital 61). Specifically, any measure "liable" to affect an MSP's media pluralism or editorial independence must also satisfy a media market concentration test, as stipulated in Article 22. On paper, this article should help partially redress the power asymmetry between media service providers (MSPs) vis-à-vis state authorities as prospective national measures potentially disruptive to media pluralism must comply with several procedural requirements[1]. Despite representing an unprecedented step forward in EU media regulation, this provision contains several potential shortcomings, which are outlined below. Before doing so, however, it is important to contextualise how this provision came about in the first place in order to understand better its raison d'être and rationale, which are outlined in Section I. Section II provides a bitesize summary of the article's main provisions, whilst Section III examines its contestable legal ba-

1. Brogi–Borges–Carlini et al. 2023.

sis. Section IV critically examines the article's main shortcomings, and the conclusion, Section V, highlights the potential added value of this provision.

1. Vivendi vs Mediaset: An important precursor to Article 21

The main aim of Article 21 is to regulate (and mitigate) the ostensible tension between market goals (viz. the freedom of establishment, harmonisation of rules, etc.), on the one hand, and non-market values (viz. media freedom, pluralism), on the other hand. Several years before the EMFA was even contemplated, these market and non-market goals came to loggerheads in a four-year legal dispute between Vivendi and Mediaset (Case C-719/18 *Vivendi SA v Autorità per le Garanzie nelle Comunicazioni*) (Fig. 1). This landmark case established an important precedent – there is a non-market value which should be protected (viz. media pluralism); however, such protection should be ensured in a proportionate manner. The following paragraphs outline how this legal dispute unfolded, as well as highlighting its parallels with Article 21 EMFA.

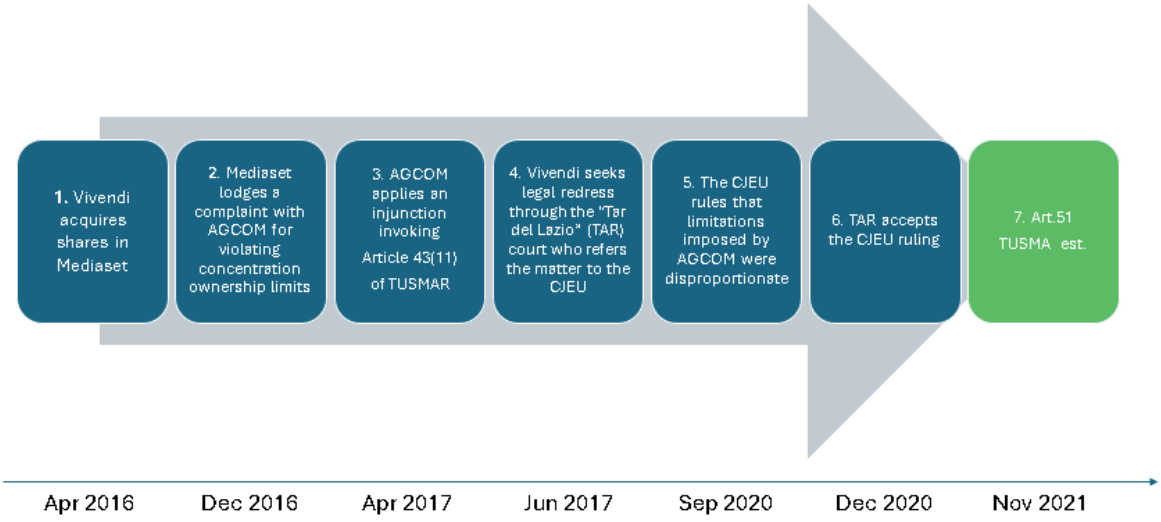

Fig. 1 — *Timeline of the Vivendi-Mediaset dispute*

In April 2016, Vivendi – a significant shareholder in the telecommunications company Telecom Italia (TIM) at the time – acquired over 20% of the shares in Mediaset. As a result of this action, a few months later, in December 2016, Mediaset filed a complaint with the Italian national media regulator, AGCOM (*Autorità per le Garanzie nelle Comunicazioni*) for allegedly breaching the thresholds[2] set out in Article 43(11) of "Testo unico della radiotelevisione" (TUSMAR[3]), which they argued would have led to Vivendi's market dominance in the Italian media and communications sector, leading to negative ramifications for media pluralism. Thereafter, AGCOM ruled in Mediaset's favour – and imposed an injunction which blocked Vivendi from buying shares in Mediaset – citing concerns that it threatened market competition and media pluralism. Vivendi then appealed to the regional Italian court, "Tar del Lazio" (TAR), which initially supported AGCOM's reasoning; however, they, nonetheless, referred the matter

2. This provision imposed two cross-sectoral ownership thresholds which prevented undertakings "from achieving turnover exceeding 40% of the overall combined revenues of the electronic communications sector in Italy while simultaneously achieving turnover exceeding 10% of the overall combined revenues of the 'Integrated System of Communications'" (Marasà 2020).
3. In effect, this provision was conceived to prevent excessive market dominance by one undertaking in the Italian media and communications sector.

to the Court of Justice of the European Union (CJEU) for further clarification[4].

The CJEU adjudged that AGCOM's injunction was disproportionate for several reasons.[5] Firstly, exceeding the absolute revenue thresholds laid down by the TUSMAR neither automatically, nor necessarily, implied control over media content. The CJEU judges sought to distinguish between content transmission and content production, which implies editorial responsibility (Case C-719/18, 2020, paras. 66-67). Indeed, the CJEU argued that TUSMAR failed to distinguish between the two, treating undertakings involved solely in transmission (in this case, Telecom Italia) as having potential influence over media content; however, for the CJEU, a sufficient justification was found wanting, arguing that, while Vivendi (a significant shareholder of Telecom Italia) may have increased its influence over the transmission of content as a result of acquiring shares in Mediaset, this did not automatically imply control over the production of content[6]. In short, AGCOM failed to consider whether exceeding the TUSMAR thresholds would have posed a genuine risk to editorial control and media pluralism in general (Case C-719/18, 2020, paras. 75-79).

As a corollary of the last point, the CJEU ruled that the fixed revenue thresholds prescribed by TUSMAR were unsuitable for detecting media pluralism risks. Under this law, the 10% threshold was effectively conceived of as an automatic risk proxy to detect threats to media pluralism. However, the Court questioned the suitability of this provision, opining that "an undertaking earn[ing] revenue equivalent to 10% of the total revenues generated in the SIC is not, in itself, an indication of the risk of influencing media pluralism" (Case C-719/18, 2020, para. 75). The Court argued that an assessment of market concentration should be more comprehensive, taking into account other contextual factors such as the impact of a given takeover on content transmission or content production, in addition to how revenues are distributed among the wide range of different markets constituting the SIC (Case C-719/18, 2020, para. 75). For example, an undertaking might have less than 10% of total revenues generated in the SIC but be heavily concentrated in one of the markets of the SIC (e.g. 40% in one market alone) which would likely constitute a plausible threat to media pluralism. Conversely, an undertaking's revenues may exceed 10% but be distributed relatively evenly (e.g. 1% across 10 different markets), which would unlikely be consequential from a media pluralism perspective (Case C-719/18, 2020, para. 75). In addition, the CJEU also questioned whether a parent company exercising 'significant influence' over an affiliate company would be consequential for media pluralism in practice (Case C-719/18, 2020, para. 77). Indeed, the bar for 'significant influence' is set relatively low – under Article 2359 of the Italian Civil Code – defined as a company being able to exercise one-fifth of the voting rights, or one-tenth, if the company has shares that are listed on the stock exchange (Case C-719/18, 2020, para. 11).

Furthermore, including revenues from both 'affiliated' and 'controlled' companies in calculating the total revenue of a given undertaking in the electronic communication sector – would, the CJEU argued, have inflated its revenue figures, thereby exaggerating its sectoral influence (Case C-719/18, 2020, paras. 75-76). Related to this last point, AGCOM's restrictive definition of the electronic communications sector (SIC) – which excluded mobile telephony and internet services – essentially had the effect of limiting the basket of different sectors comprising the "Sistema Integrato delle Comunicazioni" (SIC), which, again, would have exaggerated an undertaking's potential influence in the electronic communications sector (SIC) (Case C-719/18, 2020, paras. 71-74). In sum, the CJEU criticised Article 43 of TUSMAR's rigid thresholds for failing to assess and address the potential adverse effects on media pluralism. Instead, the Court stressed the importance of demonstrating evidence of editorial control over content rather than solely relying on rigid thresholds to assess its impact on media pluralism. Ultimately, TAR followed the CJEU's decision, highlighting that AGCOM had failed to consider various elec-

4. The decision by AGCOM, and subsequently, TAR, reflected the strict national interpretation of concentration rules which were in place at the time.
5. This is a non-exhaustive list of the CJEU's reasoning for ruling in favour of Vivendi.
6. Trevisan 2022.

tronic communications sectors, including mobile, internet-based, and satellite broadcasting services.

The outcome of this legal dispute served as an important catalyst for the revised anti-concentration rules in the "Testo Unico dei Servizi di Media Audiovisivi" (TUSMA)[7]. Under this law, identifying a dominant position based on excessive ex-ante thresholds is no longer automatic. Instead, such an evaluation is based on an ad hoc case-by-case assessment taking into account indicators symptomatic of "significant market power" (*inter alia*, revenues, the level of static and dynamic competition, convergence between sectors and markets, vertical integration of markets, control of data etc.). Therefore, rather than relying on fixed thresholds alone, regulatory authorities now have the flexibility to adjust thresholds when deemed necessary[8], taking into account the evolving multimedia landscape and other considerations[9]. It is little coincidence that the definition of 'Integrated System of Communications' (SIC) was also updated just a few months after the resolution of the Vivendi legal dispute (November 2021). The updated 'SIC', thereafter, was extended to an even broader basket of communication activities, inter-alia, print media, electronic publishing including online platforms, radio and audiovisual media services, cinema, outdoor advertising, sponsorships, and online advertising (as defined by Article 3, Para. 1, letter z of Legislative Decree No. 208/2021).

This landmark case laid the groundwork for Article 21 of the EMFA in establishing the principle that Member State measures limiting the freedom of establishment may be permitted as long as they are proportionate to obtaining some overriding objective (e.g. safeguarding media pluralism. In this case, the actions by AGCOM were found to be disproportionate as it could not be established that Vivendi's stake in Mediaset would have adverse effects on the production of content and, by extension, editorial control[10]. The Mediaset-Vivendi case elucidated two essential points: (1) national measures could potentially disrupt and fragment the functioning of the internal market by constraining the freedom of establishment, and (2) there is an important non-market value that needs protection, but such protection should be ensured in a proportionate manner[11]. The ramifications of this case highlighted the need for the EU to intervene to create a harmonised legal framework to help navigate this delicate balancing act between fostering the freedom of establishment, on the one hand, and protecting media pluralism, on the other[12].

A subsequent case, Case C-106/22 – Xella, also provides further guidance on the conditions under which limits to freedom of establishment may be justified according to EU law[13]. To summarise the main particulars of this case, the Hungarian Ministry prevented an EU-based company, *Xella Magyarorszá*, from acquiring a Hungarian company, *Janes és Társa*, on national interest grounds, claiming that it posed a threat to raw materials supplies in the construction sector – regarded as a key strategic economic sector in Hungary. The CJEU argued that such a restriction was purely of an economic protectionist nature, and this did not constitute a fundamental societal interest. The CJEU argued that restrictions to the freedom of

7. *Ibidem*.
8. *Ibidem*.
9. For more information, see Article 51 TUSMA of AGCOM's guidelines (2024) on Article 51 TUSMA (Delibera n. 66/24/CONS).
10. Both the Vivendi-Mediaset dispute and Article 51 of TUSMA inculcated the notion that media market concentration should be assessed more broadly. Indeed, assessing positions of market dominance on revenue thresholds alone does not automatically render it a threat to media pluralism. On the contrary, such an assessment should be more comprehensive, taking into account several contextual factors symptomatic of significant market power in addition to examining whether ownership ultimately has a material adverse effect on editorial control and media pluralism. In the dispute in question, while Vivendi's stake in Mediaset posed potential implications for the distribution of content, the evidence was lacking that it would have also impacted content production and thus media pluralism (Apa 2021).
11. Bonelli 2023; Brogi–Borges–Carlini et al. 2023.
12. Brogi–Borges–Carlini et al. 2023.
13. Case C-106/22, *Xella Magyarország Építőanyagipari Kft. v Innovációs és Technológiai Miniszter* EU:C:2023:568.

establishment based on purely economic grounds did not constitute a sufficient justification (Case C-106/22, para. 66). Similarly to the Vivendi-Mediaset case, the CJEU clarified the scope conditions under which a curtailment of the freedom of establishment might be lawful, reaffirming that restrictions "may be justified on grounds of public policy, public security or public health" (ORPI)[14] (Case C106/22, para. 63). Unlike the Fussl (C-555/19)[15] and Vivendi cases which established that media pluralism constitutes an 'overriding reason relating to the public interest' (C-555/19, para. 15), the CJEU ruled that this restriction was not justified on the same grounds, claiming that "the alleged loss of supply of raw materials to the construction sector did not constitute a genuine and sufficiently serious threat to a fundamental interest of Hungary's society"[16]. In short, this case reinforced the principle that a state intervention which threatens to curtail the freedom of establishment must be able to satisfy the justification (viz. ORPI) and proportionality test (later codified in Article 21(1) of the EMFA). In sum, the aforementioned cases underscore the principle that national measures should not interfere with media service providers' (MSP) freedom of establishment unless doing so would serve an overriding public interest – one of which is the protection of media pluralism. The principles laid out in this recent case, and particularly in the aforementioned Vivendi-Mediaset dispute, can be regarded precursors to Article 21 of the EMFA.

2. An overview of Article 21's main provisions

Article 21 of the EMFA establishes several procedural requirements to regulate the longstanding tension between market goals, such as the freedom of establishment, on the one hand, and non-market goals, such as media pluralism, on the other hand. The latter, an important corollary to the fundamental right of freedom of information, is enshrined in Article 11 of the EU's Charter of Fundamental Rights[17]. This article is grounded in Article 41 of the Charter of Fundamental Rights (CFR)[18] on the right to good administration, particularly Article 21's emphasis on predefined and transparent timeframes set out in advance (see, in particular, Article 21(2) and Article 21(5)). In customary EU fashion, the article incorporates the principle of proportionality as a means of reconciling these ostensibly conflictual freedoms. Article 21 aims to safeguard MSPs from national measures considered disproportionate and thus incompatible with the freedom of establishment[19]. However, the latter is not an inviolable right – indeed, this market freedom may be circumscribed if an MSP's media pluralism or editorial independence is at risk of being compromised. For example, during the "Vivendi-Mediaset" dispute, the CJEU adjudged that AGCOM's actions – namely, imposing an injunction on Vivendi's acquisition of shares in Mediaset – violated the latter's freedom of establishment. The CJEU ruled that AGCOM's injunction was disproportionate both in terms of suitability – as it could not be established that the pluralism in terms of media content production

14. The Court further added that "reasons of an economic nature in the pursuit of an objective in the public interest or the guarantee of a service of general interest may constitute an overriding reason in the public interest capable of justifying an obstacle to one of the fundamental freedoms enshrined in the Treaties" (Case C-106/22, para. 65). As Recitals 5, 8, 41 and 83 of Directive 2010/13 and the EMFA explicate, media services entail both economic and cultural components and are crucial actors in safeguarding a pluralistic information environment (C-555/19, para.3). In a similar vein, state interventions to safeguard media pluralism can also be understood as an intervention in the market by the state to safeguard fundamental interests of society such as ensuring the diversity of opinions and a pluralistic media environment, which are understood as axiomatic to the proper functioning of democracy (Recital 5 of Directive 2010/13; Recitals 2, 14, 21, 27, 32, 64 and Article 3 of the EMFA).
15. CJEU Case C-555/19 | *Fussl Modestraße Mayr GmbH v SevenOne Media GmbH.*
16. Reyntjens–Jorna 2023. See also Case C-499/23, para. 46. A.G. Szpunar (2025, February 6), Opinion of Advocate General Szpunar delivered on Case C-499/23, *European Commission v. Hungary*.
17. Brogi–Carlini–Nenadić et al. 2021.
18. Cole–Ettendorf 2023, p. 35.
19. Brogi–Borges–Carlini et al. 2023.

would be undermined – and going beyond what is necessary to achieve the purported aim of safeguarding media pluralism. As pointed out earlier, AGCOM's actions were disproportionate as the TUSMAR provision that applied rigid revenue thresholds did not adapt to evolving market conditions and changes in the competitive landscape. Additionally, the restrictive definition of 'SIC' and the skewed method for calculating total revenues (including those of both controlling and affiliated companies) were also factors taken into account by the Court. Lastly, the general presumption that holding 'significant influence' over an affiliated company would translate into material influence in a given market – thereby undermining media pluralism – could not be established (Case C-719/18, 2020, para. 77).

Summarising each paragraph in turn, Article 21(1) introduces several procedural requirements that national measures[20] must/shall adhere to. Such measures "shall be 'duly justified', 'proportionate', 'reasoned', 'transparent', 'objective' and 'non-discriminatory'" (Article 21(1))[21]. In addition, when adopting these measures, Article 21(2) – in keeping with Article 41's right to good administration CFR – stipulates that they shall adhere to timeframes set out in advance, putting MSPs on notice that a measure directly affecting them will be adopted proximately in time. In this way, MSPs are well-positioned to challenge a prospective measure deemed pernicious to media pluralism, or more specifically, the editorial independent of a media service provider (MSP). Article 21(3) states that MSPs can appeal to an independent appellate body, which may be a court[22]. As per Article 21(4), the Board and the Commission are tasked with providing opinions on such measures. Lastly, Article 21(5) grants the Board and the Commission the power to request information from the relevant national authority, as well as underlining the importance of timely and transparent communication between them[23].

The article is positive, particularly for MSPs, in so far as it provides a "sweeping constitutional protection against the future playbook of media control"[24]. Under this provision, MSPs are granted safeguards from media capture from national authorities as Member State measures must comply with several criteria that respect MSPs' media pluralism or editorial independence. Under the regulation, national regulatory bodies shall guarantee that any measures are 'reasoned, transparent, objective and non-discriminatory' – setting the normative standard at the same level as the general principles of EU law (Article 20(1)). In addition, Article 21 imposes upon Member State bodies – albeit hitherto unprescribed – timeframes and transparency requirements upon Member State bodies – a welcome development. Lastly, involving multiple bodies such as the Board and the Commission (inc. MSPs themselves) adds a further layer of accountability and oversight. Additionally, MSPs can appeal to an independent appellate body, representing an alternative/additional judicial channel in addition

20. In particular, measure "liabl" to affect the media pluralism or editorial independence of MSPs operating in the internal market.

21. In essence, the proportionality test imposes a further set of criteria that national measures must meet for them to be EMFA-compliant. It is important to stress that member states have not been handed a blank cheque; they cannot merely limit the freedom of establishment invoking media pluralism as an overriding interest. Instead, prospective measures should be 'justified', 'objective' and 'proportionate'. The latter's meaning, which is not immediately self-evident, is essentially shorthand for "…appropriate for ensuring the attainment of the objective in question and not go beyond what is necessary to attain that objective", as stated in the *Polbud – Wykonawstwo* case (C-106/16, EU:C:2017:804, para. 52). See also *Sky Österreich* (C-283/11).

22. Article 21(3) is the most significant provision as it grants MSPs the right to appeal national measures.

23. Para. 1 of Article 21 lays out a general principle, namely, that Member State measures should not undermine media and market freedoms unless it is justified and proportionate. Para. 2-5 contain the nitty gritty of the provision, with Para. 2 containing an ex-ante protection for MSPs by imposing transparency obligations upon Member States measures captured by Article 21. Conversely, Para. 3-5 contain ex post safeguards for MSPs in so far as several bodies including the Board, Commission, and, crucially, MSPs themselves, have oversight powers. Brogi–Borges–Carlini et al. 2023.

24. Tambini 2023.

to national courts whose political independence may have been compromised. However, this situation raises two important questions: Firstly, will there be a designated body to handle appeals or a state of affairs wherein different bodies are assigned on an ad-hoc basis? Secondly, will these bodies have the legal expertise and apply the same level of rigour as national 'courts of *law*' – a term that is notably absent in the final adopted text[25]. Although extending the scope of bodies permitted to enforce Article 21 might be desirable from a practical perspective, it risks fragmenting the levels of scrutiny and legal standards applied across Member States, thus ultimately undermining legal certainty.

3. Assessing the legal basis of Article 21

Article 114 TFEU is invoked as the legal basis for the EMFA in general and Article 21 in particular[26]. Loosely speaking, the main aim of Article 114 TFEU is to prevent regulatory fragmentation, and thus, an uneven playing for businesses, which is disruptive to the functioning of the internal market. The Vivendi-Mediaset case illustrates how disruptive national measures can be for media service providers operating in the internal market. In this respect, and as per the principle of conferral laid out in Article 5 TEU, the EU can only act within the competences stipulated in the EU treaties. The CJEU, through its jurisprudence, has a purely interpretative function, and does not have the power to grant the EU new, explicit competences to act (see also Art. 267 TFEU). Notwithstanding these considerations, Article 114 TFEU's measures for approximation serve as a plausible legal basis for Article 21, which introduces measures to facilitate the harmonisation of Member State laws, regulations or administrative actions pertaining to the functioning of the internal market. Article 21 of the EMFA is, after all, an attempt to provide a minimum set of requirements that all member states must adhere to when implementing national measures. However, Article 21 goes one step further by regulating measures 'liable' or 'likely' (the terminology employed in the article) to affect media pluralism. This might appear to be a contentious element of the provision as Article 114 TFEU is about establishing the internal market, which may, prima facie, only seem tangentially related to a pluralistic media environment.

However, as Article 114(3) TFEU elucidates, non-market objectives such as "public health, safety, environmental protection and consumer protection" may be sought as measures of approximation[27]. Indeed, it is typical for internal market pieces of legislation to pursue (besides market liberalisation) further legitimate public interests, for example, by setting out common standards to regulate the sector and imposing common minimum rules to protect legitimate public interests such as media pluralism and independence[28]. Media service providers and recipients can, as a result, provide and receive such services within a properly functioning internal market in which cross-border regulatory cooperation is enhanced, and the principles of media pluralism and independence are respected, in line with Article 11 of the Charter of Fundamental Rights[29]. Indeed, CJEU case law[30] (e.g., CJEU judgment in Case C-283/11 *Sky*

25. The term "court of law" was included in the draft text proposed by the European Parliament. Brogi–Borges–Carlini et al. 2023.
26. Brogi–Borges–Carlini et al. 2023.
27. Before the TFEU was introduced, CJEU jurisprudence established the principle that obstacles to the free movement of goods could be justified if they pursued legitimate objectives such as public health, and consumer protection but they had to be proportionate to the objective pursued (most notably the "Cassis de Dijon" (1979) case which set a precedent for justifying restrictions on the free movement of goods for the protection of public health; see also: *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* (1979).
28. Malferrari 2025.
29. *Ibidem*. See, for instance, recitals 8, 21, 28, 34 and 46 of the EMFA Regulation.
30. See also C-260/89, *Elliniki Radiophonia Tileorassi AE v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas* (1991). In this case, the CJEU highlighted that a monopoly is "unacceptable not only in the context of the freedom to provide services but also to ensure a range of voices are available to the public" (European Parliament 2015).

Österreich GmbH v Österreichischer Rundfunk[31]) reaffirms that the EU can pursue non-market objectives through Article 114 TFEU[32]. As alluded to above, in the "Vivendi-Mediaset" case, it was recognised that pursuing pluralism within democratic societies may represent an objective of general interest that may justify the restriction of freedom of establishment. In this case, Advocate General Sánchez-Bordona opined that protecting information pluralism (stated in Article 11 of the Charter of Fundamental Rights of the European Union) constituted an overriding reason in the public interest[33]. This position also chimes with the views of several scholars who argue that legislation can favour non-market objectives even if it curtails the four freedoms[34]. Indeed, the implicit objective of Article 21 of the EMFA is to ensure national regulatory frameworks are harmonised to support enterprises' freedom of establishment across the whole EU. However, in doing so, national rules should take into account specific non-market objectives, such as media pluralism. Several scholars also argue that fundamental rights may fall within the remit of Article 114[35]. This is confirmed in CJEU jurisprudence (see for ex. Sky Oesterreich and PL v. EP and Council "copyright Directive")[36]. As the freedom of expression, and its corollary, media pluralism, are considered one of the fundamental rights of the EU, as per Article 11 CFR, a further argument can be made that Article 114 TFEU provides a legal basis for Article 21[37]. The legal basis for the EMFA in Article 114 TFEU is also endorsed by the legal service of the Council of the EU (that is, the legal advisor to the organ comprising the Member States of the EU). According to the same, the crux of the matter is whether a provision has the capacity to "obstruct fundamental freedoms and thus have a direct effect on the functioning of the internal market or to cause significant distortions of competition" (Council, 2022/0277 (COD)). In this regard, Article 21 clearly satisfies these conditions. National differences in rules on media mergers, and the lack of legal certainty it engenders, clearly threaten MSPs' freedom of establishment, as evidenced by the drawn-out "Vivendi-Mediaset" dispute. Had this happened in another Member State, it is reasonable to argue that matters would have unfolded quite differently, and Vivendi would have been allowed to acquire shares in Mediaset. Indeed, Article 21 precisely aims to avoid situations of this kind – namely, regulatory fragmentation of the internal market and legal uncertainty for MSPs' cross-border operations.

Several observers have also identified Article 36 TFEU as providing a possible legal basis for this provision. Article 36 TFEU allows Member States to derogate from the internal market principles in certain circumstances, such as protecting public health, life, and the environment. The fact that there is no explicit mention of fundamental rights such as freedom of information, and its corollary, media pluralism therein, should not be interpreted as an impediment as the protection of fundamental rights is a general objective of public interest[38]. (see Schmidberger v. Austria, Case C-112/00, 2003, and Omega Spielhallen- und Automatenaufstellungs GmbH v. Oberbürgermeisterin der Bundesstadt Bonn, Case C-36/02, 2004). However, the EMFA is about services and not goods (which is the object of Article 36 TFEU)[39].

A somewhat more tenuous argument has been put forward that Article 167 TFEU might provide a legal basis for Article 21 of the EMFA in so far as it strengthens the EU's commitment to promoting

31. Without indulging into the particulars of the case, the CJEU essentially held that the freedom of establishment could justifiably be curtailed if media pluralism, deemed an overriding public interest, was under threat.
32. See also Wållgren 2016.
33. Court of Justice of the European Union (2019, December 18), Advocate General's Opinion in Case C-719/18, *Vivendi SA v Autorità per le Garanzie nelle Comunicazioni*, 18 December 2019.
34. de Witte 2012; Kosta 2015; Wållgren 2016, p. 29.
35. E.g.w Kosta 2013, p. 25, found in Wållgren 2016, p. 30.
36. Malferrari 2025.
37. Brogi–Carlini–Nenadić et al. 2021.
38. Malferrari 2025.
39. *Ibidem*.

cultural diversity and supporting the cultural and creative sectors (e.g. the audiovisual sector). Article 167 TFEU, in effect, grants the EU a limited competence to intervene in the field of culture only in order to bring the "common cultural heritage to the fore" (viz. European identity and culture). However, there are several reasons why Article 167 TFEU can be ruled out as a legitimate legal basis for Article 21 of the EMFA. Firstly, Article 167 is merely a supporting competence of the EU, as stipulated by Article 6 TFEU, which means that the EU can only support, coordinate or supplement Member States' actions, but they cannot impose the harmonisation of Member States' national laws. Indeed, this is explicated in Article 167(5), which states that the EU "shall adopt incentive measures, excluding any harmonisation of the laws and regulations of the Member States". Moreover, as Article 167(5) makes plain, the EU's intervention is limited to so-called 'incentive measures' – which can be understood as non-binding instruments to motivate or encourage Member States to undertake particular policy actions[40]. Lastly, the scope of Article 167 TFEU is limited to the audiovisual sector; therefore, the EU would not have the competence to legislate in other media sectors, regardless.

Several observers have raised legitimate concerns about the potential incongruence of EMFA with existent EU legislation, such as the AVMS Directive 2010/13/EU, which encourages Member States to pursue cultural policy measures while respecting cultural diversity[41]. However, Article 21's procedural requirements, arguably, make it harder for Member States to adopt these measures as they must comply with both legislative regimes. There is also a potential incompatibility issue between this regulation and the AVMS Directive, leaving some room for Member States to prioritise cultural matters (inc. local ones) over purely internal market considerations. In particular, Article 13(1) – which relates to the promotion of European works – grants Member States limited discretion on how best to encourage the distribution of European content whilst respecting local cultural diversity[42]. However, under the EMFA, there is a risk that pursuing national cultural policies to support local media production could be deemed 'discriminatory' or 'non-objective', potentially falling foul of Article 21(1). Notwithstanding these concerns, there is, on balance, a clear market-oriented logic to the article, namely, facilitating MSPs' freedom of establishment and freedom to provide services by means of harmonisation of national measures. As a result, the legal basis for Article 21 may be justifiably anchored to Article 114 TFEU. In addition, there is a clear precedent deriving from existing EU legislation (e.g., Directive 2010/13/EU) and CJEU case law (e.g., Vivendi-Mediaset) indicating that the EU may legislate on matters related to media pluralism[43].

4. A critical examination of Article 21

Notwithstanding the clear added value of this provision, which represents an unprecedented step forward in the EU's media regulatory framework,

40. A paradigmatic example is the Creative Europe Programme which provides EU funding (e.g. grants, co-financing) and networking opportunities to encourage cross-border collaboration between Member States in cultural and creative sectors.

41. SAA et al. 2023; *Open letter to European institutions regarding the impact of EMFA regulation proposal on cultural audiovisual policies*, Brussels, 2023, June 9). In a nutshell, this directive encourages member states to pursue cultural policy measures whilst respecting cultural diversity. For instance, Recital 69 of the directive states that member states "should, where practicable, promote the production and distribution of European works and thus contribute actively to the promotion of cultural diversity". See also Recital 19 which states that "this Directive does not affect the responsibility of the Member States and their authorities with regard to the organisation – including the systems of licensing, administrative authorisation or taxation – the financing and the content of programmes. The independence of cultural developments in the Member States and the preservation of cultural diversity in the Union therefore remain unaffected." This affords member states some flexibility when organising their audiovisual systems taking into account their variegated local, socio-cultural and economic settings.

42. AVMS Directive – Recital 5; *Open letter to European institutions...*, cit.; SAA et al. 2023.

43. It is difficult to disentangle economic from non-economic considerations particularly given the nature of media service providers which are "as much cultural services as they are economic services" (Recital 5 of the AVMS Directive).

several potential pitfalls threaten to undermine its legal effectiveness and enforceability. Firstly, the circumstances under which the Commission should communicate an opinion are unclear[44] . Unlike the Board, whose intervention appears non-negotiable (Article 20(4) stipulates that the Board '*shall*' issue an opinion), the Commission's role is ostensibly discretionary as evinced by the phrase "the Commission *may* [or not] issue its own opinion on the matter"[45]. The former is more affirmative language than the latter, imposing a clear obligation to act. The wide degree of discretion granted to the Commission, instead, enhances the provision's legal uncertainty as it is unclear under what conditions the Commission would or should intervene. The Commission could, however, bind its own discretion by setting out guidelines delineating the criteria for deciding whether to intervene or not. It is also unclear what happens in instances of disagreement between the Board and the Commission and which of the two 'opinions' carry more weight. This uncertainty also applies to disagreements between national courts and the hitherto unspecified appellate body[46]. In other words, there is a risk of cascading and conflicting opinions from various organs, which might create uncertainty regarding which opinion should be followed. In addition, enhanced clarity regarding the specific roles and responsibilities of the national bodies, MSPs, the Board, the Commission, and 'other regulatory authorities' would improve the provision's effective implementation and enforcement[47]. Clarification will, presumably, be provided by the CJEU as well as published EU guidelines on Article 21. It is, furthermore, unclear which governing body is ultimately responsible for monitoring (non-) compliance of this provision: the appellate body, Board, Commission or courts? That said, based on the reading of Art. 267 TFEU, it can be reasonably assumed that the competent national court (if a court of last instance) may refer a question to the CJEU to give a ruling thereon. Moreover, it is also still not clear what the repercussions are (if any) in case the Board fails to lodge an opinion, which itself, lacks legal enforceability. Crucially, there appear to be no sanctioning regimes in place for instances of non-compliance[48].

The consistency of language employed in Article 21 could also be improved. In Article 20(1), for example, the term '*liable* to affect' is used, whereas in Article 20(4) and 20(5), the term '*likely* to affect' is preferred (italics added). The former carries a more objective legal connotation, whereas '*likely* to affect' leaves room for more subjectivity. This begs the question: Does the decision on 'liability' or 'likelihood' lie with the regulatory authority of a Member State, appellate body, Board, European Commission or national and/or supranational court?[49] The wording and the order in which the Article is composed implies that Member States would initially be responsible for determining whether a proposed measure is 'liable to affect' media pluralism of media service providers operating within the internal market whereas Article 20(4) Article 20(5) implies that both the Board and European Commission would be co-responsible in deciding its likely 'impact'[50]. As a corollary to the previous point, the scope of this provision is potentially overreaching as it is not entirely clear when a national measure would be deemed liable (Article 20(1)) or likely to impact the functioning of the internal market for media services (Article 20(5)). Indeed, the threshold for impact is set rather low as, arguably, all national measures have some impact

44. Brogi–Borges–Carlini et al. 2023. This paper builds on many of the points that were raised in the Centre of Media Pluralism and Media Freedom's study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) titled: "The European Media Freedom Act: media freedom, freedom of expression and pluralism" (Brogi–Borges–Carlini et al. 2023).

45. Brogi–Borges–Carlini et al. 2023, italics added.

46. *Ibidem*. Although it can be reasonably expected that the competent national court's judgments will be binding on the appellate body and judgments stemming from the CJEU will hold the most weight.

47. Cole–Ettendorf 2023, p. 7; Brogi–Borges–Carlini et al. 2023.

48. *Ibidem.*

49. Brogi–Borges–Carlini et al. 2023.

50. *Ibidem.*

on MSPs operating in the internal market, even to a minimum extent[51]. In addition, it is worth noting that Article 21(1) includes measures 'liable to affect media pluralism or the editorial independence' of MSPs (italics added), which, arguably, extends the scope even further, as editorial independence is just one facet of a broader phenomenon[52]. While the scope of this provision is potentially far-reaching, it should be noted that there are additional criteria that need to be satisfied – a given measure must be necessary, justified, and proportionate. The forthcoming guidelines on this article and the other articles of the EMFA will likely be crucial in delineating the provision's scope.

The following section dissects and critically examines each paragraph of Article 21, beginning with the first paragraph. In essence, Para. 1 of Article 21 subjects national measures to three conditions. These measures shall not negatively impact: (1) media pluralism (2) the internal market, and (3) they must be 'proportional', 'duly justified', 'reasoned', 'transparent', 'objective' and 'non-discriminatory'. It is interesting to note that the original European Commission (EC) text was wider in scope. Initially, 'any measure liable to affect the internal market' would have triggered Article 21(1). However, in the finally adopted text, its scope was limited to measures liable to affect 'media pluralism or editorial independence of media service providers operating in the internal market'. The objective of this article is now explicitly stated, helping to clarify its scope. The EP's proposed amendments were the most potentially far-reaching, including the "provision" of media services within its remit, which implies the more content-oriented aspects of media services. Limiting the scope to the operating arm of MSPs is welcome as it is evidently not the intention of this article, which is more about setting out rules related to the ownership structure of MSPs, falling under the more operational aspects of media service providers (see Recital 60 for more)[53].

Moreover, omitting the word "provision" from the final text could help to reduce the risk of a potential conflict between Article 21 of the EMFA and preexisting EU legislation, in particular, Article 167 TFEU, which is about supporting the creation of content (e.g. artistic and literary creation, including in the audiovisual sector, to promote cultural diversity). Indeed, several observers in the audiovisual sector had voiced concerns that the original EC proposal text might create an incongruence between Member States measures aimed at safeguarding cultural diversity, including at the local and national level, in fulfilment of Article 167 TFEU, and Member States measures in compliance with Article 21 EMFA[54]. Compared to the final text, Recital 38 of the European Parliamentary amendments was more explicit in this regard, stating that "the requirement to communicate such measures does not aim to affect national measures implementing Directive 2010/13/EU insofar as they do not affect media pluralism and editorial independence, national measures taken pursuant to Article 167 TFEU, national measures taken for the purpose of promoting European works or national measures which are otherwise governed by State aid rules". At the very least, Recital 61 of the finally agreed text clarifies that Article 21 should not undermine the implementation of State-aid measures[55]. Nonetheless, it remains to be seen how the interplay of these laws would play out in

51. *Ibidem.*

52. Brogi–Borges–Carlini et al. 2023.

53. Recital 60 helps clarify what are the intended types of measures that Art. 21 will help to regulate: (i) Limiting ownership of media by other sectors (e.g., Vivendi-Mediaset); (ii) decisions on licensing, including revoking or making renewal difficult for MSPs, and (iii) decisions related to the authorization or prior notification of MSPs.

54. "The implementation of a number of cultural policies stemming from national legislations adopted in procedural fairness and fully consistent with Article 167 TFEU could potentially be disputed by media service providers' unilateral interpretation of their disproportionality or unjustifiability…protecting media pluralism and media independence must not, inadvertently or otherwise, lead to undermining cultural diversity" (*Open letter to European institutions...*, cit.).

55. In the final text, Recital 61 and Recital 73 include a positive commitment. Recital 61 states that "Without prejudice to the application of the Union's competition and State aid rules […]" and Recital 73 states that "this Regulation should not affect the application of the Union's public procurement and State aid rules".

practice. If, for example, Member States wish to implement measures in the audiovisual sector in order to preserve and promote national identity – which is a "right" of Member States enshrined in Article 4(2) TEU and compliant with Article 167 TFEU – this may inadvertently fall foul of Article 21 EMFA as such measures might, arguably, threaten media pluralism by favouring national content or narratives, via, for example, higher quotas, which, in turn, might marginalise local or minority voices. However, as a counterargument to this, measures to protect or promote national customs, culture and identity can, perhaps, be justified as an overriding reason in the public interest[56] provided that such measures are proportionate and carefully balanced against other EU values such as safeguarding media pluralism or market freedom, which must themselves be carefully balanced, and vice versa (internal market rules are expected to take cultural diversity into account). Indeed, this is made explicit in para. 4 of Article 167 TFEU, which states that "[t]he Union shall take cultural aspects into account in its action under other provisions of the Treaties, in particular in order to respect and to promote the diversity of its cultures."

While the narrowing in scope of Article 21 in the final text is also a positive step, it is arguably too broad. Article 20(1) refers to 'media service providers operating in the internal market' and not just the service arm of their operations[57]. The phrase 'Media service providers *operating* in the internal market' (italics added) entails a far-reaching scope, encompassing a broader scope of activities beyond the mere provision of media services, including the administration, management, finance, corporate structure, etc. As Cole and Etteldorf aptly point out[58], the question of scope is especially important given that Article 20(3) establishes a direct appeals process involving an 'appellate body'[59].

Article 21(2) stipulates that media regulators must adopt clear timeframes in adopting these measures. While not explicitly referencing Article 41 of the Charter of Fundamental Rights (CFR), which concerns the right to efficient administration and timely decision-making processes, Article 21(2) is clearly conceived with Article 41 CFR in mind. Notably, the text 'preparatory phases' has been omitted from the final text, which poses the risk of not providing MSPs – and other relevant parties directly affected by a national measure – with sufficient time to examine a prospective measure in detail. Moreover, the lack of clarity on what constitutes a 'sufficient timeframe' poses a potential issue in terms of legal certainty. The European Parliament's (EP) proposed amendments are more explicit in this regard, stipulating that "such timeframes shall be of sufficient length to ensure that such measures and their consequences can be properly considered and that media service providers directly affected can provide feedback on them"[60] (formerly Article 20(2) of the EP's proposed amendments). Interestingly, this detail moved to Recital 60 in the adopted text. However, as EU legal scholars have pointed out, recitals are non-binding, which might give Member States more wriggle room to hastily adopt measures to bypass scrutiny.

Article 21(3) establishes a new complaint mechanism granting MSPs the right to appeal to an independent 'appellate body', which represents an additional, or alternative recourse to national courts whose political independence might be in disrepute[61]. However, this inter-institutional arrangement raises two important questions: Firstly, will there be a designated body consistently assigned to handle complaints or

56. E.g. Council of the City of Stoke-on-Trent and Norwich City Council v B&Q plc, C-169/91, EU:C:1992:519, para. 11; See also Fachverband der Buch – und Medienwirtschaft v LIBRO Handelsgesellschaft mbH, C-531/07, EU:C:2009:276, paras. 32-34.

57. Brogi–Borges–Carlini et al. 2023.

58. Cole–Ettendorf 2023.

59. Cole–Ettendorf 2023, p. 35; Brogi–Borges–Carlini et al. 2023.

60. In addition, Recital 38 of the European Parliament (EP) text states that "national measures…should be communicated to media service providers well in advance of their adoption in order to prevent possible disruptions and allow media service providers enough time to assess the impact of such measures on media pluralism and editorial freedom".

61. Brogi–Borges–Carlini et al. 2023.

an ad-hoc arrangement where different bodies are allocated on a case-by-case basis? Secondly, will these hitherto undesignated bodies match the rigour and legal expertise of national courts (of *law*) (italics added) – a word notably absent from the final provision?[62]. Indeed, this article risks diluting the standards expected of the legal authority summoned to enforce Article 21 EMFA. In this respect, The EP's proposed amendments were more comprehensive, explicitly stating that the body must be a "court of *law*". However, the latter has been omitted from the finally agreed text, posing the risk that these bodies will not meet the expected legal standards. Article 41 on the right to good administration (CFR), as well as Article 47 on guaranteeing the right to an effective remedy and to a fair trial by an independent and impartial tribunal (CFR), should, however, help to quell these concerns. The same applies to Article 19 TEU, which states that bodies (e.g. 'courts' or 'tribunals') adjudicating matters within the scope of Union law should meet the requirements of effective judicial protection (viz. judicial independence and impartiality) (*Associação Sindical dos Juízes Portugueses v Tribunal de Contas* – Case C-64/16, 2018, para. 36). However, these general principles of EU law cannot compensate for the fact that the article still lacks important details regarding the appeals process, such as time limits for filing appeals, and the standard of review to be applied by the appellate body. This lack of procedural clarity could result in delays, uncertainty, and inconsistency in the resolution of appeals. The EP's focus on guaranteeing "sufficient funding" for these bodies, originally in the Article, has been moved to Recital 60. This modification poses the risk of diluting the standard and quality of appellate bodies expected to oversee such complex matters. Moreover, in the final text, the authority of the Board has been diluted slightly. In contrast, in the EP's proposed amendments, the Board was conferred an augmented role, with their opinions taken into consideration by the appellate body when handling appeals. As a corollary of the last point, the final text now grants the Board the right of initiative to issue opinions, which was not included in the original proposal. However, crucially, it does not state explicitly whether these opinions should be considered by the appellate body.

As per Article 21(4), MSPs can request an opinion from the Board and the Commission can also lodge an opinion. However, this poses the risk of 'opening the floodgates' to vexatious requests overburdening the Board (e.g., MSPs might request opinions from the Board for matters unrelated to media pluralism concerns). This right should have been circumscribed so that only the most serious violations are considered[63]. Recital 61 in the final text helps mitigate this risk slightly, specifying that all national remedies must be exhausted before seeking the Board's opinion. Under Article 21(5), the Board and EC may request relevant information from a national authority that has an obligation to provide it without undue delay. The proposed amendments by the European Parliament would have provided greater legal certainty by specifying the information that should be disclosed by national authorities. The language in these amendments is clearer, opting for "shall" instead of "may", indicating a requirement for the Board to issue an opinion. While the final text includes the obligation to provide information without "undue delay," which is welcome, it remains somewhat vague. This information should also have been made publicly available to enhance scrutiny and oversight from other interested parties.

5. Conclusion: A counterfactual highlighting the added value of Article 21 EMFA

To conclude, Article 21(1) EMFA codifies the principle that was already becoming crystallised in CJEU case law – namely, that measures taken by Member States cannot undermine the functioning of the internal market (e.g. freedom of establishment) unless such measures are justified (i.e. it is an "overriding reason in the public interest" e.g. media pluralism) and proportionate (e.g. such measures are suitable for achieving the purported aim of protecting editorial independence or media pluralism, more generally). On top of this, such measures satisfying the scope condition of Article 21(1) must also meet several procedural requirements (e.g. transparency obligations). The rationale for this is to allow various stakeholders to scruti-

62. *Ibidem*.

63. ERGA 2023.

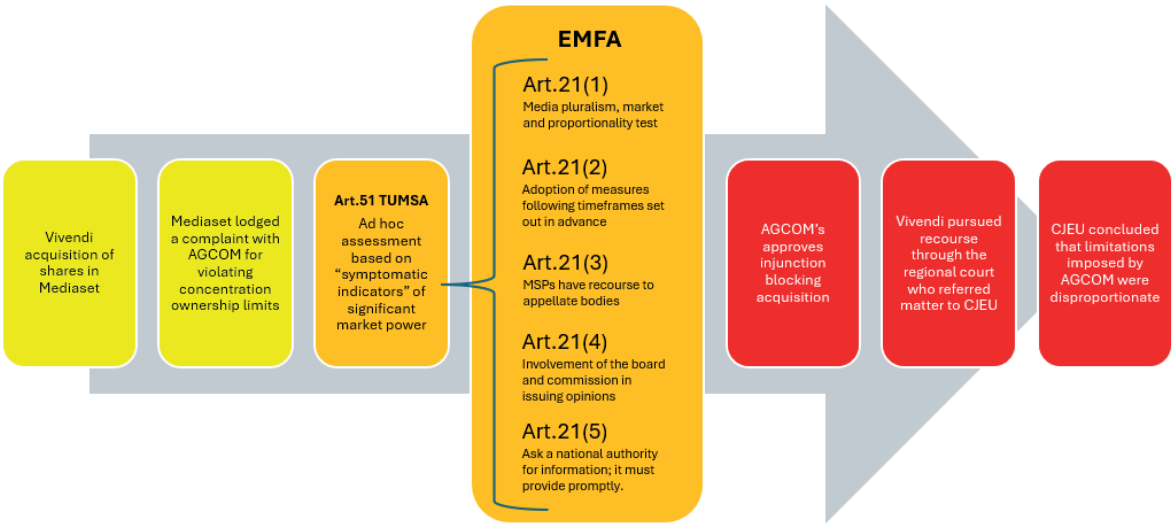

Fig. 2 — *A counterfactual of the Vivendi-Mediaset case in a post-EMFA scenario*

nise prospective measures and appeal to those they regard as deleterious to their market freedoms or media pluralism. The powers of scrutiny and oversight also extend to the Board, Commission, the appellate bodies, national courts, and needless to say, the CJEU. However, it is not yet clear what are the precise roles and responsibilities of these different organs, and nor is it clear what is the interplay between them. Indeed, eventual guidelines on this article and the EMFA, in general, will likely be crucial in determining its effectiveness.

To demonstrate the provision's added value, a counterfactual example of the Vivendi-Mediaset legal dispute is presented below to illustrate how the case might have panned out in a post-EMFA scenario (Fig. 2). Firstly, as per Article 21(1), AGCOM's decision to enforce an injunction would have been subject to a media pluralism test taking into account market considerations and a proportionality test. As per 21(2), AGCOM would have been obliged to set out a pre-established time frame without undue delay before any measure (e.g. an injunction) was introduced, thus allowing affected parties, in this case, Vivendi, to scrutinise the action proposed by AGCOM. Under Article 21(3), both Vivendi and Mediaset would have the right to appeal before an independent appellate body in addition to their right to seek legal redress from a court, which might help to prevent these legal disputes from escalating to the judiciary and the CJEU as a last resort (thereby avoiding the stages highlighted in red below). Under Article 21(4), both Vivendi and Mediaset would have been able to request an opinion from the Board (which has its own right of initiative) and the European Commission. Lastly, under Article 21(5), the Board and the Commission may request relevant information from a national authority which is obliged to provide it without "undue delay". The purpose of the European Media Freedom Act is, therefore, to avoid media-related enterprises, in this case, Vivendi, from being exposed to disproportionate State measures in so far that they fail the market and media pluralism test. AGCOM's action failed both tests for violating Vivendi's freedom to conduct business freely within the internal market and there was insufficient evidence that Vivendi's acquisition of shares in Mediaset would have influenced the production of media content, which implies editorial control. Notwithstanding, however, the article's added value in terms of granting media service providers several powers of foresight, oversight and enhanced legal certainty by means of harmonisation, legal certainty remains an issue that could undermine its legal effectiveness and enforceability.

References

E. Apa (2021), *Sic et non: nel caso Vivendi la Corte di giustizia censura le incongruenze della disciplina italiana a tutela del pluralismo dell'informazione*, in "MediaLaws", 2021, n. 1

AGCOM (2024), *Delibera n. 66/24/CONS*: Adozione delle linee guida volte alla verifica dell'esistenza di posizioni di significativo potere di mercato lesive del pluralismo, ai sensi dell'art. 51, comma 5, del D. Lgs. 8 novembre 2021, n. 208

M. Bonelli (2023), *Personal communication*, 6 June 2023

E. Brogi, D. Borges, R. Carlini et al. (2023), *The European Media Freedom Act: Media freedom, freedom of expression and pluralism*, Policy Department for Citizens' Rights and Constitutional Affairs, 2023

E. Brogi, R. Carlini, I. Nenadić et al. (2021), Chapter 1: *EU and media policy: conceptualising media pluralism in the era of online platforms. The experience of the Media Pluralism Monitor*, in "Research Handbook on EU Media Law and Policy", Edward Elgar Publishing, 2021

M.D. Cole, C. Etteldorf (2023), *Research for CULT Committee – European Media Freedom Act - Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, 2023

B. De Witte (2012), *A Competence to Protect: The pursuit of non-market aims through internal market legislation*, in P. Syrpis (ed.), "The Judiciary, the Legislature and the EU Internal Market", Cambridge University, 2012

ERGA (European Regulatory Group for Audiovisual Media Services) (2023), *European Media Freedom Act (EMFA) ERGA recommendations for EMFA trilogues*, 2023

European Parliament (2015), *Briefing: Press freedom in the EU. Legal framework and challenges*, April 2015

A. Giannaccari (2020), *La contesa Mediaset-Vivendi tra libertà di stabilimento e pluralismo informativo. Tanto tuonò che piovve*, in "Mercato Concorrenza Regole", 2020, n. 3

O. Grandinetti (2022), *La tutela del pluralismo nel nuovo Testo unico sui servizi di media audiovisivi*, in "MediaLaws", 2022, n. 2

V. Kosta (2015), *Fundamental rights in EU internal market legislation*, Hart Publishing, 2015

E. Marasà (2020). *The CJEU rules that certain anti-concentration limits set forth by Italian legislation for the protection of media pluralism are incompatible with EU law*, in "MediaLaws", 21 September 2020

L. Malferrari (2025), *Personal communication*, 21 January 2025

M. Orofino (2020), *SIC... transit gloria mundi. La Corte di giustizia dichiara le soglie asimmetriche del sistema integrato delle comunicazioni incompatibili con la libertà di stabilimento (CGUE 5a Sez., Sent. 3/9/2020, causa C-719/18, Vivendi SA v. Autorità Garanzie nelle Comunicazioni e Mediaset")*, in "Osservatorio Costituzionale", 2020, n. 6

T. Reyntjens, A. Jorna (2023), *Reading the ECJ's Xella judgment in its constitutional and institutional context*, Oxford Law Blogs, October 2023

SAA (Society of Audiovisual Authors) et al. (2023), *Joint Position Paper on the European Media Freedom Act*, 24 April 2023

G. Tambini (2023), *The EU is taking practical measures to protect media freedom. Now we need theory*, Centre for Media Pluralism and Freedom, 5 September 2023

M. Trevisan (2022), *La concentrazione nei media e il pluralismo informativo in Italia*, in E. Brogi, M. Mariani (eds.), "Temi di diritto dell'informazione e della comunicazione", Key Editore, 2022

M. Wållgren (2016), *Exploring the Outer Limits of Article 114 TFEU – towards a general power? An analysis of non-market objectives and "measures having as their object the establishment and functioning of the internal market"*, Master's Thesis in European Union Law, Uppsala Universitet, 2016

S. Weatherill (2011), *The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a "Drafting Guide"*, in "German Law Journal", vol. 12, 2011, n. 3

R. Zaccaria, A. Valastro, E. Albanesi (2021), Diritto dell'informazione e della comunicazione, CEDAM, 2021

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0229 • articolo sottoposto a peer review • pubblicato in anteprima il 2 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Matteo Trevisan

The governance framework of the European Media Freedom Act

The present contribution deals with the governance framework of the recently adopted European Media Freedom Act (EMFA). After providing an introduction on the structures and mechanisms envisaged by previous European regulatory settings, from the 1989 Television without Frontiers Directive (TwFD) to the revised 2018 Audiovisual Media Services Directive (AVMSD), the article proceeds with an analysis of the governance and cooperative infrastructure designed for the new 2024/1083 Regulation, with a special focus on the measures designed for guaranteeing the independence of the actors involved, provided in Chapter III of the Act (Framework for regulatory cooperation and a well-functioning internal market for media services).

EMFA – European Board for Media Services (EBMS) – National Regulatory Authorities (NRAs) – Independence Institutional framework – Regulatory cooperation and convergence

Il sistema di governance del Regolamento europeo sulla libertà dei media

L'articolo si propone di analizzare il sistema di governance del recente Regolamento europeo sulla libertà dei media (EMFA). Partendo da un'introduzione sulle strutture e i meccanismi istituiti attraverso le precedenti normative, dalla Direttiva Televisione senza frontiere del 1989 (TSF) alla revisione della Direttiva sui Servizi di Media Audiovisivi del 2018 (AVMSD), il contributo procede con un'analisi dell'infrastruttura di governance e di cooperazione che emerge dal nuovo Regolamento 2024/1083, con un'attenzione specifica alle misure volte a garantire l'indipendenza degli attori coinvolti, configurate nel Capitolo III del Regolamento (Quadro di riferimento per la cooperazione normativa e per il buon funzionamento del mercato interno dei servizi di media).

EMFA – Comitato europeo per i servizi di media (EBMS) – Autorità indipendenti di regolamentazione (NRAs) Indipendenza – Quadro istituzionale – Cooperazione e convergenza normativa

The Author is Associate Researcher at the Centre for Pluralism and Freedom (CMPF) of the European University Institute (EUI)

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

Summary: 1. Introduction: the path towards a European framework for media services. – 2. The governance structures of the revised AVMSD: Article 30 and the European Regulators Group for Audiovisual Media Services (ERGA). – 3. Governance and cooperative structures of the European Media Freedom Act: Independent Media Authorities (Art. 7), The European Board for Media Services (Artt. 8-13), and Regulatory cooperation and convergence (Artt. 14-17). – 4. Reflections on the independence of the core institutional actors involved in the enforcement of EMFA. – 5. Considerations on the Board and the national authorities' action under EMFA Art. 22.

1. Introduction: the path towards a European framework for media services

On 7 May 2024, two years after the publication of the Proposal on September 16, 2022 , the European Media Freedom Act (EMFA) was published in the Official Journal of the European Union[1]. This new and sector-specific regulatory framework represents a turning point for media freedom and pluralism in the European Union, providing a new and relevant set of tools and safeguards.

While adopted in a relatively short period of time, the final text is the result of a process spanning more than three decades, characterised by an increasing convergence on technological, economic, and industrial aspects. This dynamic was soon addressed by the European institutions, which intervened with the adoption of the Television without Frontiers Directive (TwFD) in 1989[2]. Designed in a time when the transborder transmission of television programs was expanding through cable and satellite technologies, the Directive was aimed at protecting the free provision of television services in the internal market, while concomitantly harmonising a set of requirements linked to important public interest objectives[3].

The unfolding potential and developments in the audiovisual sector in the following years prompted the European institutions to further evolve the regulatory framework. First amended in 1997, the TwFD was recodified in the 2007 Audiovisual Media Services Directive (AVMSD) and, subsequently, in its 2010 and 2018 versions. As a matter of fact, the AVMSD struck "a balance between promoting the free circulation of audiovisual content, protecting consumers, and upholding public policy objectives"[4], coming to represent "a cornerstone of media policy at European level"[5].

1. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).
2. Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities.
3. Another effort to harmonise the European television sphere was the European Convention on Transfrontier Television (ECTT), which entered into force in 1993. However, this was not "inspired by the EU's free-market orientation", but "embedded in the cultural policy tradition of the Council of Europe and sought to encourage the free flow of information". See Katsirea 2014.
4. Brogi–Borges–Carlini et al. 2023, p. 25 ss.
5. *Ivi*, p. 25.

This whole process, and the last two steps particularly, was characterised by the increased interplay of a wide range of institutional and non-institutional stakeholders, which accompanied the development of a pan European framework for the governance of the audiovisual media sphere. At the centre of the process were the national regulatory authorities (NRAs), entrusted with the national transposition of the EU Directives, and their cross-national harmonisation through the European Regulators Group for Audiovisual Media Services (ERGA).

Following the 2022 Commission Proposal for a European Media Freedom Act, this institutional architecture underwent significant innovation, both on the side of the governance structures and the cooperation mechanisms aimed at the supranational coordination. This has ultimately matured into Chapter III of the new EMFA Regulation, and specifically in Section 1 (Independent Media Authorities), Section 2 (European Board for Media Services), and Section 3 (Regulatory Cooperation and Convergence).

Based on these crucial novelties, the aim of the present contribution is to analyse the governance design of the EMFA, with particular attention to the requirements of independence foreseen for the major actors involved. The article will proceed as follows: first, it will provide an analysis of the governance and cooperative mechanisms already defined in the 2018 AVMSD, while contextualising the role and characteristics of its major institutional players. Second, it will investigate the novelties foreseen in Sections 1-3 of Chapter III of the EMFA Regulation, dedicating special attention to the governance system of the newly-established European Board for Media Services (EBMS). Third, it will highlight the main points of contention related to Chapter III that have emerged since the beginning of the legislative process, up to the adoption of the final text, opening a reflection on the side of independence and enforceability.

2. The governance structures of the revised AVMSD: Article 30 and the European Regulators Group for Audiovisual Media Services (ERGA)

The ultimate basis for the governance design of the European Media Freedom Act is Article 30 of the revised AVMS Directive. Located in Chapter XI ("*Authorities and Regulatory Bodies of the Member States*"), the article places the NRAs at the centre of the entire AVMSD structure, specifying their characteristics, their functions, and setting the framework for their cooperation[6].

While the origins of Article 30 can be traced back to the 1990s, specific criteria for the independence of pan European architecture started to be postulated more clearly only in the late 2000s, especially in light of the emerging evidence of regulatory capture[7] in some of the newer Member States, which had the potential to undermine the effective implementation of the Directive[8]. As a last step, the 2018 AVMSD provided that NRAs shall be "legally distinct from the government and functionally independent of their respective governments and of any other public or private body", that they "shall exercise their powers impartially and transparently", "shall not seek or take instructions from any other body", and must be provided with "adequate financial and human resources and enforcement powers"[9]. As it will

6. Art. 30 (b) of AVMSD refers to "national regulatory authorities or bodies in the field of audiovisual media services with primary responsibility for overseeing audiovisual media services, or where there is no national regulatory authority or body, by other representatives as chosen through their procedures". As such, a National Regulatory Authority may not necessarily coincide with a media authority.
7. Regulatory capture occurs when the regulatory agency aimed at regulating and protecting an industry in the public interest, is in turn subjected to commercial and political interference. The risk is the distortion of its supervisory power in favor of the interests of the industry which is supposed to be regulated. See Stigler 1971.
8. A first discussion on independence began in 1998 following the European Commission's "Oreja Report"; however, it was only with the 2005 Proposal for revising the TwFD that preliminary measures were suggested, while an explicit reference to "independent regulatory bodies" had to wait until the 2010 AVMSD. See Oreja 1998.
9. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative

be further explained in the following paragraphs, these provisions were designed without prejudice to the power of Member States to define the procedures for the appointment and dismissal of the respective NRAs' Boards.

In terms of cooperation structures, Article 30 specifically built on the provisions of the Commission Decision of 3 February 2014[10], which marked the establishment of the European Regulators Group for Audiovisual Media Services (ERGA). Designed as an advisory body to the European Commission (hereinafter, the "Commission") to face the cross-border distribution of audiovisual services and the challenges posed by on-demand ones, the setting up of ERGA constituted a significant step change, as it offered the systematisation of a new supranational governance structure aimed at fostering advice and cooperation between NRAs, as well as "a direct channel to the Commission and the chance to form common position and voice common concerns"[11]. Notably, it also served to complement such a framework with a body provided with a different membership compared to both the Contact Committee inherited by the TwFD[12] and the European Platform of Regulatory Authorities (EPRA)[13].

The creation of ERGA – the first output of which was, precisely, a study on the independence of NRAs[14] – represented an essential passage towards the definition of Article 30 and the related institutional framework. This ultimately resulted in a tripartite governance mechanism involving the European Commission, the Member States, and national regulators, with their confrontation being disposed of in two organisms: the Contact Committee, characterised by the participation of Government ministers or senior civil servants, and chaired by the Commission; and ERGA, composed of representatives of NRAs, with the Commission being downgraded from chair to participant in the meetings[15].

3. Governance and cooperative structures of the European Media Freedom Act: Independent Media Authorities (Art. 7), The European Board for Media Services (Artt. 8-13), and Regulatory cooperation and convergence (Artt. 14-17)

As provided by Section 1[16] of the European Media Freedom Act – hereinafter "the Act" – the application of Chapter III[17] is conferred to the NRAs, whose definition activities are bound to the requirements already set out in Article 30 of the AVMSD.[18] In addition, in the text it has been ensured that they are provided with "adequate financial, human and technical resources", along with the ability to request data and information that are "proportionate and necessary" for the tasks defined in Chapter III.

action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

10. Commission Decision of 3 February 2014 on establishing the European Regulators Group for Audiovisual Media Services, C(2014) 462.
11. Broughton Micova 2021, p. 279.
12. As per the TwFD and the subsequent AVMSD (Art. 29), the Contact Committee is participated by representatives of the national government ministries, which makes it unsuitable in terms of ensuring independence. See Woods 2018.
13. In fact, EPRA Board Members "are not representatives of their respective authorities, but individuals elected through nomination, performing their duties on a philanthropic basis (…)". Moreover, "its statutes expressly prohibit the adoption of common positions or declarations". See Cappello 2019, p. 15. Moreover, it has also to be underlined that EPRA is not only participated by EU Member States.
14. See Erga 2015.
15. This is something to be considered as highly relevant in terms of ERGA's independence from both Member States, commercial interests, and the Commission. See Woods 2018.
16. Independent Media Authorities, Art. 7.
17. Framework for regulatory cooperation and a well-functioning internal market for media services.
18. As already anticipated, Art. 30 (b) AVMSD does not exclude that an NRA could be an authority or body other than an audiovisual media regulator.

The structure, governance system, and core functions of the newly established European Board for Media Services (EBMS) are provided in Section 2 (Artt. 8 to 13), which restored most of the provisions foreseen by the 2014 Commission Decision on establishing ERGA, and the 2018 revised Directive. Article 8 establishes that the EBMS will replace and succeed ERGA through a targeted amendment of Directive 2010/13/EU (Art. 30b), while Article 9 (Independence of the Board) provides that it shall act in "full independence", meaning "neither seek nor take instructions from any government, institution or body". Compared to the AVMSD, Rules of Procedure will have to be adopted "in consultation" (and not anymore "in agreement") with the Commission; importantly, these shall also include measures against conflicts of interest of the members of the Board.

The composition and governance of the EBMS are detailed by Article 10 EMFA (Structure of the Board). As well as in the case of ERGA, the Board will be composed of representatives of the regulatory authorities, and provided with one vote each for decisions to be deliberated in a two-third majority ballot[19]. The Chair and a Vice-Chair will be elected amongst the Board's members, with the term of office of the Chair being of one year, renewable once. A representative of the Commission will be also designated, however without voting rights, while the Board "should be able to set up" a Steering Group, invite experts and (in agreement with the Commission) permanent observers to attend its meetings. Moreover, a Commission-based Secretariat aimed at administrative and organisational support is also to be established according to Article 11, along with a consultation mechanism (Article 12) with relevant representatives in the case of dealing with matters beyond the audiovisual media sector.

Article 13 (Tasks of the Board) lists the core functions of the Board. The EBMS shall provide technical expertise to the Commission, promote cooperation and the effective exchange of information, experience and best practices among NRAs. Save for the cases where the Board can act on its own initiative – a relevant novelty, compared to the initial 2022 proposal – it shall provide opinions on technical and factual issues to be initiated upon request of, or delivered in consultation with, the Commission. Among others, opinions might concern measures that are likely to affect the internal market (such as, for example, media concentrations), cases of disagreement between NRAs, as well as national measures concerning media services from outside the Union.

Chapter III concludes with section 3, specifically dedicated to regulatory cooperation and convergence. It details procedural rules for structured cooperation and mutual assistance between NRAs (Art. 14), it regulates requests for enforcement of obligations of video-sharing platform providers (Art. 15) and defines the specific cases for which the Board shall assist the Commission for the issuing of guidelines (Art. 16). Notably, it also provides with specific provisions for the coordination of measures concerning media services from outside the Union that prejudice or present a serious and grave risk of prejudice to public security (Art. 17).

4. Reflections on the independence of the core institutional actors involved in the enforcement of EMFA

It can be argued that the above-mentioned provisions have positively boosted the institutional structures in support of a cooperative and independent pan European media framework. While confirming most of the AVMSD stipulations[20], EMFA offers a broadened scope of action, entrusting the newly-created EBMS with a wide-ranging set of competences which extend to printed press, online media, as well as to the relationship with online platforms (Article 18). Importantly, it also provides a detailed framework for cooperation and mutual assistance between NRAs, involving an accelerated procedure for particular cases[21].

At the same time, the process and subsequent debate leading to the approval of the Regulation have unearthed significant problematic points,

19. Where a Member State has more than one national regulatory authority or body, a joint representative shall be elected.

20. Such as the requirements of independence for NRAs, the governance structures envisaged for ERGA, including the nomination system based on a two-thirds majority ballot, and the Commission-based Secretariat.

21. See Art. 14 (6) of the Act.

which from the initial proposal to the final text have found only limited solutions. For what specifically concerns the infrastructure defined in Chapter III, criticism was mainly expressed in relation to the independence of the EBMS from the Commission[22], and the independence of NRAs from Member States[23], which might have consequences for the independence of the EBMS as well, and the effectiveness of the whole EMFA structure[24].

Regarding the first consideration, several stakeholders pointed to the cumbersome involvement of the Commission in both the design of the EBMS, its tasks, and the Secretariat. In fact, if considering the 2022 Proposal, the tasks were largely subjected to the request or the agreement of the Commission, implying potential leverage from its part[25]. Besides, the Board was not provided with the right of initiative at its own discretion, whereas the Secretariat was designed as a Commission-based administrative branch, which also raised concerns[26].

Although in the final text the role of the Commission can be still considered rather relevant[27], some major adaptations have been provided. First, the Board's Rules of Procedures are now to be adopted "in consultation with the Commission", and not "on the Commission's proposal" like in the AVMSD, or "in agreement with" as per the EMFA initial text. Moreover, the agreement of the Commission, which in the Proposal was largely needed before any action to be potentially undertaken by the Board, has been in general transformed into a requirement of consultation. This adds to the fact that the Board has been granted with the possibility to provide opinions on its own initiative[28], which is to be considered as a major improvement, compared to the initial proposal. Not least, Article 11(2) EMFA specifies that "the secretariat shall act on the sole instructions of the Board regarding its tasks under this Regulation", subsequently limiting the concern expressed against the Commission's leverage. In these terms, the final text appears certainly more balanced.

The second consideration to be developed here questions the sufficiency of the safeguards for the independence of NRAs, which might also affect the EBMS. As a matter of fact, the NRAs will be the core bodies for the implementation of the Regulation in the single EU countries: subsequently, their potential dependency on political power might negatively interfere with the implementation and effectiveness of the whole regulatory infrastructure. As argued by Bayer, "if an authority is captured, and serves the particular interests of a ruling government, as in illiberal systems, then these powers and resources serve that capturing power, and further aggravate the rule of law situation within the Member States, and on the affected media market. Their switchboard function threatens with the unintended result that instead of implementing the European principle of media freedom and pluralism at the national level, they

22. See Erga 2022; Cole–Etteldorf 2023; Aer 2023; Article 19 2023.

23. See Bayer–Cseres 2023.

24. See Cmpf 2023.

25. See Efj 2023; Article 19 2023; Cole–Etteldorf 2023.

26. As argued by Cole–Etteldorf 2023, the Secretariat did not appear to be designed as a mere administrative support structure. In consequence of that, some of the stakeholders involved in the consultation process expressed their preference for an agency-based Secretariat. See Cmpf 2023, Article 19 2022.

27. Consultation is requested for opinions related to cooperation between NRAs, requests for enforcement measures in the event of disagreement between NRAs, and national measures concerning media services from outside the Union. Moreover, the Board is asked for opinions upon request of the Commission, something that, according to Bayer, is to be considered as "a clear informal pressure on national measures". See Bayer 2024, p. 141.

28. The Board can opine on its own with respect to "regulatory or administrative measures which are likely to significantly affect the operation of MSPs in the internal market, in accordance with Article 21(4)"; "draft assessments or draft opinions of national regulatory authorities or bodies, in accordance with Article 22(5)"; "media market concentrations which are likely to affect the functioning of the internal market for media services, in accordance with Article 23(1)" (in such cases, the opinions can be initiated also at the request of the Commission or upon a duly justified and reasoned request of a media service provider that is individually and directly affected).

will either block the process or – even worse – one bad apple can put the whole barrel in danger"[29]. The potential of these risks are corroborated by the results of the Media Pluralism Monitor (MPM)[30], evidencing how politically-compromised procedures for the governance and funding of NRAs can have a clear effect on the impartiality and effectiveness of their action. While the MPM indicator called "Independence and effectiveness of the national regulatory authorities" signals a low level of risk Europe wide, the 2024 MPM implementation outlined that one more country, Greece, enters the high-risk band for NRA's independence, along with Hungary, Poland, and Turkey. Moreover, the most recent implementations of the MPM detected a deteriorating trend with specific regards to the independence of governance structures and procedures of the national media authorities.

In this context, it is essential to recall the process that led to the provisions for independence defined in Art. 30 of the AVMSD and, subsequently, in Art. 7 of the EMFA. As anticipated, the very first output of ERGA was a 2015 report on NRAs' independence, based on a questionnaire answered by the same regulators. The report certified significant fragmentation across national systems on several dimensions related to NRAs' independence (i.e., appointment procedures, the mandate of the Head of the Board, and incompatibility rules), and delineated some essential recommendations and principles in light of the revision of the AVMSD[31]. However, the report also notably underscored the impossibility, at that time, to come up with an agreement on more specific safeguards for the 2018 AVMSD, implying that "the notion of independence is understood very differently among Member States"[32]. Moreover, Member States have proved, over the years, rather reluctant in further fine tuning the provisions for independence of the NRAs, recurring to their cultural competence[33]. Hence, albeit the final text of the revised AVMSD has ultimately integrated some essential and innovative provisions, in these terms[34], more detailed and comprehensive considerations on incompatibility and procedures for appointments and dismissals were not included. Least of all, no reference to that is found in the Rules of Procedures that have been adopted in 2019 by ERGA in the aftermath of the revised Directive[35].

The point is relevant because EMFA, which formally updates the AVMSD, does not intervene as well in the internal governance of the NRAs. As a matter of fact, the provisions on conflict of interests that are to be defined in the forthcoming EBMS' Rules of Procedure will shape the governance of the Board, but not the internal governance of national regulators, again granting to Member States a certain degree of discretion. Especially in national contexts where blatant regulatory capture has emerged, this might prove detrimental,

29. See Bayer 2024, p. 135.
30. The MPM is a risk-based assessment tool aimed at identifying the risks to media pluralism and media freedom in the 27 Member States of the European Union and the candidate countries.
31. Besides a generic reference that NRAs' mandate should be free from conflict of interest, the final recommendations of the report clearly suggested that the institutional frameworks of Member States "shall" guarantee independence notably by "open and transparent nomination and appointment procedures; ensuring that the dismissal of the NRA's Chair or Board Members is based on transparent and objective grounds as prescribed in the relevant law/regulation; introducing incompatibility and conflict of interest rules in their national laws". See Erga 2015, p. 62.
32. Notably, the report underlined that, "at least at [that] moment", an agreement on the fact that appointment procedures should be open and transparent, was the highest level of harmonisation that could be achieved. Moreover, the answers to the questionnaire significantly highlighted that "a large majority of NRAs consider[ed] their procedures as "open and transparent", even though in some cases political parties [were] clearly represented within the Board". *Ibidem*.
33. See Cappello 2019.
34. See preamble in recital 53 of the 2018 AVMSD, introducing the requirement of "functional independence", complementing that of "formal independence". However, no interpretation on what constitutes "functional independence" has been provided by the CJEU, so far. See also paragraph 5 of Art. 30 of the 2018 AVMSD.
35. See *Rules of Procedure of the European Regulators Group for Audiovisual Media Services*, ver. 10.12.2019.

as generic criteria could be easily circumvented by creating only formally compliant governance structures. Moreover, while it is expected that the requirements on financial support to NRAs as instated in Article 7 of the EMFA will support the NRAs' ability to deal with the increased competences and tasks, there might still be a chance for Member States to condition the activity of regulators based on the financial input that will be provided to them.

Therefore, an argument remains on whether an opportunity has been missed to update the AVSMD criteria in a way that would have ensured substantial independence, especially in light of the increased responsibilities entrusted to the NRAs. An extensive study on the NRAs' independence, similar to that compiled in the process of revision of the AVMSD, would certainly have been beneficial to re-evaluate the state of affairs for the media authorities at the EU level, while further exploring innovative solutions aimed at ensuring autonomy and independence.

5. Considerations on the Board and the national authorities' action under EMFA Art. 22

When it specifically comes to the ability of the Board and the NRAs to carry out the tasks entrusted to them by EMFA, one could consider the potential outcomes of the assessment of media market concentrations provided for by Article 22 EMFA, that requires a specific evaluation of the impact of media concentrations on media pluralism and editorial independence (the so-called "media plurality test").

In terms of institutional competences, the provision entrusts the assessment to the "independent media authorities" or "independent national bodies" "to which the Member States have already entrusted the function of 'National Regulatory Authority' (NRA) for the implementation of the (EU) Audiovisual Media Services Directive (AVMSD)"[36]. This suggests that the bodies to be designated for such assessment will mainly be audiovisual regulators, although it is not excluded that Member States could assign the media plurality test to a National Competition Authority – especially in national cases where media regulatory bodies do not exist (i.e., Spain), or where Member States have already embedded the evaluation of media concentrations within the competition procedure. One should also not overlook the possibility that more than one media authority could be designated as responsible for carrying out such an assessment.

Albeit relevant research has underlined that NCAs have been "historically rather reluctant to take media plurality into account as per the "*unquantifiable metric* of plurality"[37], with EMFA the fact that a NCA, instead than a media authority, would be entrusted with such a task does not actually appear problematic, as far as the NCA in question proves its independence from external influences, and is able to execute the parallel procedures foreseen by Art. 22 EMFA, the national competition law, and Art. 21(4) of Regulation EC 139/2004[38]. As to the possibility that more than one media authority would be entrusted with the media plurality assessment, this seems a rather unlikely case, given the well-established European audiovisual regulatory situation, and also if considering the national bodies already involved in the ERGA framework. Nonetheless, it has been highlighted as a potential contingency in the case of Poland, where the creation of the National Media Council has made unclear the attribution of competences vis-à-vis the National Broadcasting Council, also raising "possible structural conflict"[39].

With specific regard to the procedural design, it is worth analysing in detail how the media pluralism test relates to competition mechanisms. Based on EMFA Art. 22, it proves considerably

36. Manganelli–Mariniello 2024, p. 166.

37. Parcu–Brogi–Verza et al. 2022, p. 241.

38. "Plurality of the media" was already part of the national legitimate interests that Member States could safeguard according to Art. 21(4) of Regulation EC 139/2004), although optionally. See Parcu–Brogi–Verza et al. 2022. The combined reading of Art. 22 EMFA, Recital 66, and Art. 21(4) of Regulation EC 139/2004) suggests that the formerly optional clause for competition authority to consider plurality of the media, becomes binding. See Cole–Etteldorf 2024.

39. See Sznajder 2023.

laborious to foresee the outcomes of a media market concentration in the case of conflicting results between the parallel media and economic assessments envisioned by the Regulation. It can be argued with certainty that a merger negatively affecting both media pluralism and competition will be prohibited by respective authorities, while a merger with positive effects in terms of pluralism, and not impacting competition rules, will be approved. Similarly, it can be safely assumed that a concentration that is approved by the media plurality test, but disapproved by the competition assessment, will be blocked – or subjected to conditions – by the competition authority. This has been, for example, the case of the takeover of Métropole Télévision (M6) by the Bouygues group, which ultimately withdrew the acquisition plan after the *Autorité de la Concurrence*, regardless of the positive assessment from the media regulator Arcom, imposed further conditions[40].

However, it is not straightforward what the outcome could be when a media concentration negatively affects media pluralism, and not competition[41]. While it is foreseen that the EBMS' peer review system will be activated[42], the opinion to be deliberated by the Board remains non-binding, raising not only the question "on which procedure would ultimately prevail", but also some reservation on the resolutive power of the EBMS vis-à-vis such potential elements of conflictuality. Considering such a situation, Sznajder has argued that the whole process would likely result "in a return to status quo, where competition law and its economic assessment take precedence, no matter what", ultimately questioning the rationale behind the media pluralism test.

On a different line, Cole and Etteldorf have underlined that, in the case of divergent assessments, "it must be assumed that a merger can be prohibited independently of each procedure or made subject to conditions (without the EMFA itself specifying possible legal consequences)". This would imply that media pluralism-related considerations will play a somewhat binding effect, as per the coactive role of Art. 22(1) subpara. 1 EMFA and Recital 66, and Art. 21(4) of the Merger Regulation.

In the final instance, the combined reading of such provisions suggests that media pluralism-related considerations could in any case block a merger affecting pluralism, regardless of a different outcome from the national competition procedure. Otherwise said, for a media market transaction to be approved, both the media plurality test and the competition assessment must be cleared. In such a context, one should also consider that authorities are requested to cooperate so as to ensure the objectives of the Regulation[43], while the EBMS is expected to play a major role in guiding any potential procedural conflictuality towards a positive resolution.

More certainty is instead detected when considering the specific national cases where the intervention of the Ministry is needed for the NRAs' decisions to take effect. As a matter of fact, EMFA Art. 22 will abolish the possibility of governmental intervention and ministerial override in media concentration and pluralism-related assessments, reserving it only to independent national authorities[44].

References

AER - Association of European Radios (2023), *AER Position on the proposal for a European Media Freedom Act*, 2023

Arcom (2022), *Notice of April 29, 2022 to the Competition Authority on the proposed takeover of the Métropole Télévision group by the Bouygues group*, 2022

40. See Arcom 2022.
41. See Sznajder 2023.
42. The national regulators involved shall then take "utmost account" of the opinion of the Board, and provide a justification in case the opinion is not followed.
43. See by analogy European Court of Justice, Judgment of the Court (Grand Chamber) of 4 July 2023, *Meta Platforms Inc and Others v Bundeskartellamt*.
44. Manganelli–Mariniello 2024.

Article 19 (2022), *European Media Freedom Act: The European Board for Media Services. ARTICLE 19's concerns on the proposal of the European Board for Media Services*, 2022

J. Bayer (2024), *Digital Media Regulation within the European Union. A Framework for a New Media Order*, Nomos, 2024

J. Bayer, K. Cseres (2023), *Without Enforcement, the EMFA Is Dead Letter*, in "Verfassungsblog: On Matters Constitutional", 2023

E. Brogi, D. Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, Study PE 747.930, 2023

S. Broughton Micova (2021), *The Audiovisual Media Services Directive,* in "Research Handbook on EU Media Law and Policy", Edward Elgar Publishing EBooks, 2021

M. Cappello (ed.) (2019), *The independence of media regulatory authorities in Europe*, IRIS Special, European Audiovisual Observatory, 2019

CMPF - Centre for Media Pluralism and Media Freedom (2023), *Feedback on the proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU*, 2023

M.D. Cole, C. Etteldorf (2024), *The European Media Freedom Act unpacked*, European Audiovisual Observatory, 2024

M.D. Cole, C. Etteldorf (2023), *Research for CULT Committee – European Media Freedom Act - Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, 2023

EFJ - European Federation of Journalists (2023), *EFJ position paper on the EMFA Proposal*, 2023

ERGA - European Regulators Group for Audiovisual Media Services (2022), *ERGA position paper for the Open Public Consultation*, 2022

ERGA - European Regulators Group for Audiovisual Media Services (2015), *ERGA Report on the Independence of NRAs*, ERGA (2015)11

I. Katsirea (2014), *The Television Without Frontiers Directive*, in K. Donders, C. Pauwels, J. Loisen (eds.), "The Palgrave Handbook of European Media Policy", Palgrave Macmillan, 2014

A. Manganelli, M.L. Mariniello (2024), *Media Concentration and Plurality Test*, in "Rivista italiana di informatica e diritto", 2024, n. 2

M. Oreja (1998), *The Digital Age: European Audiovisual Policy. Report from the High Level Group on Audiovisual Policy*, 1998

P. Parcu, E. Brogi, S. Verza et al. (2022), *Study on media plurality and diversity online – Final report*, European Commission: Directorate-General for Communications Networks, Content and Technology, Publications Office of the European Union, 2022

G.J. Stigler (1971), *The Theory of Economic Regulation*, in "The Bell Journal of Economics and Management Science", vol. 2, 1971, n. 1

M. Sznajder (2023), *European Media Freedom Act and its implications for both merger control and media pluralism: the Polish perspective*, 2023

L. Woods (2018), *Revision of Audiovisual Media Services Directive – Video-sharing Platforms*, 2018

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0221 • articolo sottoposto a peer review • pubblicato in anteprima il 29 mag. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Camilla Lobascio

Micro-targeting politico e protezione dei dati personali. Il Regolamento (UE) 2024/900

L'ampio ricorso agli strumenti digitali promette di rendere più efficienti i processi decisionali, ma solleva interrogativi rilevanti circa l'impatto di tali tecnologie sui diritti e sulle libertà fondamentali. Ciò avviene in particolare in materia di protezione dei dati personali, specie quando i dati sono usati a fini politici, come nelle campagne elettorali, momento in cui gli utenti possono essere esposti a contenuti mirati in condizioni di vulnerabilità e senza piena consapevolezza della natura sponsorizzata del messaggio. Tali dinamiche rischiano di influenzare opinioni e scelte politiche in modo potenzialmente manipolatorio. In risposta a queste criticità, il Regolamento (UE) 2024/900 ha introdotto norme armonizzate sull'uso di tecniche di targeting e diffusione dei messaggi pubblicitari che implicano il trattamento di dati personali nel contesto della pubblicità politica online. Tuttavia, il regolamento si concentra sulla pubblicità politica, senza intervenire su altre forme di comunicazione potenzialmente manipolatorie, come le campagne di disinformazione o di guerra ibrida, che sfruttano algoritmi e sistemi di raccomandazione per ottenere visibilità. Fra le piattaforme digitali interessate dalla normativa, Google ha deciso di sospendere la pubblicità politica, mentre Meta non ha ancora adottato una posizione ufficiale. Resta il rischio che la normativa, pur nata con finalità di tutela, possa finire per restringere lo spazio del dibattito politico online.

Micro-targeting – Datificazione – Elezioni – Privacy – Regolamento 2024/900 – Diritti neurali

Political micro-targeting and data protection regulation: Regulation (EU) 2024/900

The widespread use of digital tools promises to make decision-making processes more efficient, but raises relevant questions about the impact of such technologies on fundamental rights and freedoms, in particular with regard to the protection of personal data, especially when data are used for political purposes, as in election campaigns, when users may be exposed to targeted content in vulnerable conditions and without full awareness of the sponsored nature of the message. Such dynamics risk influencing opinions and political choices in a potentially manipulative way. In response to these critical issues, Regulation (EU) 2024/900 introduced harmonised rules on the use of targeting techniques and dissemination of advertising messages involving the processing of personal data in the context of online political advertising. However, the regulation focuses on political advertising, without intervening on other potentially manipulative forms of communication, such as disinformation or hybrid warfare campaigns, which exploit algorithms and recommendation systems to gain visibility. Among the digital platforms affected by the regulation, Google has decided to suspend political advertising, while Meta has not yet adopted an official position. The risk remains that the legislation, although born with protective purposes, may end up restricting the space for online political debate.

Micro-targeting – Datification – Elections – Privacy – Regulation 2024/900 – Neural rights

L'Autrice è dottoranda di ricerca presso il Dipartimento di Giurisprudenza dell'Università degli studi di Macerata

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* Part II - a cura di Elda Brogi

Sommario: 1. La mercificazione dei dati. – 2. La trasformazione della sfera pubblica e politica come effetto della diffusione della rete. – 3. Sistemi di raccomandazione, *neural rights* e impatto sulle decisioni - 4. *Targeting* politico e protezione dei dati personali, tentativi di soluzione europei. – 5. Il regolamento europeo in materia di targeting e trasparenza della pubblicità politica (2024/900). – 6. Conclusioni.

1. La mercificazione dei dati

È ampiamente riscontrata la diffusione di un modello di business[1] che prevede l'erogazione di servizi a titolo gratuito, senza la previsione di un corrispettivo pecuniario, subordinatamente all'acquisizione del consenso per il trattamento dei dati personali degli utenti. Tale modello risulta particolarmente prevalente nelle interazioni online, pur non essendo esclusivamente ad esse circoscritto, ed è stato favorito dal progresso delle nuove tecnologie, che forniscono tecniche sempre più pervasive e sofisticate di raccolta, monitoraggio e sfruttamento dei dati personali. La fornitura di beni e servizi costituisce infatti un'occasione preziosa per accedere alle potenzialità economiche dei cosiddetti *big data*[2]. L'*Autorité de la Concurrence* in Francia e il *Bundeskartellamt* in Germania hanno congiuntamente sottolineato come la creazione di valore sia strettamente connessa allo sviluppo di nuove tecniche in grado di estrarre "informazioni preziose da enormi quantità di dati (spesso non strutturati)". In questo contesto, i *big data* risultano strettamente collegati ai *big analytics*, ovvero alla capacità dei sistemi informatici di affrontare problemi complessi attraverso l'analisi di grandi volumi di dati grazie all'uso di algoritmi avanzati[3]. I dati personali costituiscono ricchezza e alimentano dunque l'economia digitale. A conferma di ciò, il d.lgs. 4 novembre 2021, n. 173 ha introdotto all'interno del Codice del Consumo (d.lgs. 6 settembre 2005, n. 206) il Capo I *bis* denominato "*Dei contratti di fornitura di contenuto digitale e di servizi digitali*". L'art 135-*octies* (*Ambito di applicazione e definizioni*), si occupa della fattispecie dello scambio di contenuti/servizi con dati personali a fronte del pagamento di una somma di denaro. Il GDPR riconosce che l'interessato (o consumatore) si trova in una posizione di svantaggio nel rapporto contrattuale, motivo per cui il Capo III del regolamento gli attribuisce specifici diritti, tra cui la possibilità di gestire e controllare la diffusione delle proprie informazioni personali. Nonostante ciò, lo sfruttamento economico dei dati personali rimane una questione problematica: il *footprint* digitale degli individui è gestito dalle grandi *digital companies*, che lo utilizzano per influenzare opinioni e comportamenti in molteplici ambiti. Questa dinamica è aggravata dalla formazione di oligopoli, che non solo limitano la concorrenza ma consolidano il potere delle piattaforme, riducendo

1. Per una definizione di modello di business si può far riferimento alla descrizione di G. Donna: "Le numerose definizioni proposte, pure differenziandosi sul piano lessicale, convergono nell'identificare nel modello di business l'illustrazione di come un'azienda intende creare valore. 'Business models are stories that explains how enterprises work … to deliver value to customers, entice customers to pay for value and convert those payments to profits'" in Donna 2018.
2. Thobani 2019.
3. Gobbato 2019.

ulteriormente il margine di controllo dei consumatori sui propri dati e sulla loro stessa esperienza digitale[4].

Nel mercato dei dati costituito da piattaforme online e motori di ricerca, la mercificazione delle persone, o la loro riduzione a materia prima, come afferma S. Zuboff, si riferiscono al fenomeno in cui le persone sono trattate principalmente come risorse da sfruttare per fini economici o di controllo[5]. Non sorprende che sia stato evidenziato come sia del tutto legittimo affermare che le informazioni (e quindi i dati), oltre a supportare e ottimizzare gli scambi economici e le transazioni convenzionali, stiano assumendo il ruolo di un vero e proprio fattore di produzione, comparabile a terra, capitale e lavoro[6].

Ma quali sono le implicazioni giuridiche della mercificazione associata alla *datification*[7] delle persone? Quali sono le conseguenze legali quando la mercificazione è incentivata, in maniera più o meno consapevole, dall'uso diffuso dei social network e dei motori di ricerca? Risulta impossibile al momento fornire una risposta definitiva ai quesiti posti, poiché la complessità del fenomeno della mercificazione associata alla *datification* delle persone è oggetto di dibattito e riflessioni giuridiche in evoluzione costante. La trasformazione dei dati personali in beni di valore economico, e la conseguente mercificazione degli individui attraverso le loro tracce digitali, solleva molteplici questioni di stampo sia legale che etico che non possono essere pienamente risolte con una normativa univoca. In aggiunta a ciò è utile ricordare che, nel regolamentare la tecnologia, è difficile non imbattersi nel cosiddetto dilemma di Collingridge[8]. Questo fenomeno descrive la situazione in cui, dal momento dell'emergere di un'innovazione tecnologica alla sua regolamentazione, passa molto tempo a causa di una certa esitazione dei regolatori, i quali non agiscono tempestivamente per mancanza di informazioni più specifiche sul funzionamento della tecnologia di riferimento. Pertanto, nel momento in cui tali informazioni diventano disponibili, le normative rischiano di essere già obsolete, poiché non più allineate con i progressi tecnologici. Ci troviamo, infatti, di fronte sia ad un problema di mancanza di informazioni (il che significa che gli impatti non possono essere facilmente previsti fino a quando la tecnologia non è ampiamente sviluppata e utilizzata dalla popolazione) sia a un problema di potere (il controllo o il cambiamento diventano difficili quando la tecnologia è ormai profondamente radicata). Le iniziative regolamentari adottate finora dall'Unione europea, sebbene apprezzabili, non forniscono ancora una risposta completa alle sfide poste dalla mercificazione dei dati personali, incentivata, spesso inconsapevolmente, attraverso l'uso diffuso dei social network e dei motori di ricerca. Le tecnologie emergenti e l'economia basata sui dati, in particolare i modelli di business che si fondano sulla raccolta e l'analisi delle attività online degli utenti, hanno richiesto vari interventi da parte dell'Unione europea per promuovere la libera circolazione dei dati personali, garantendo al contempo una protezione agli individui. A tal proposito, la normativa eurounionale, attraverso il GDPR, il *Digital Services Act* e il *Digital Markets Act*, il *Data Act* e il *Data Governance Act*, mira a facilitare il flusso libero dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali. Questi interventi sono stati necessari perché ai fenomeni descritti si affianca una sorveglianza di massa continua e pervasiva, resa

4. Morace Pinelli 2024.
5. Zuboff 2019.
6. Califano 2021.
7. Per una definizione interdisciplinare di *datification* si può far riferimento a quella fornita da Mejias–Couldry 2019: "Datafication is not just the making of information, which, in one sense, human beings have been doing since the creation of symbols and writing. Rather, datafication is a contemporary phenomenon which refers to the quantification of human life through digital information, very often for economic value. This process has major social consequences. Disciplines such as political economy, critical data studies, software studies, legal theory, and – more recently – decolonial theory, have considered different aspects of those consequences to be important. Fundamental to all such approaches is the analysis of the intersection of power and knowledge".
8. Genus–Stirling 2018, pp.61-69.

possibile dalla diffusione capillare di Internet e dall'attività delle piattaforme digitali predominanti. Queste raccolgono e analizzano enormi quantità di dati, rafforzando il controllo sugli utenti e influenzando dinamiche economiche, sociali e politiche. Questo sistema solleva importanti questioni giuridiche relative alla tutela della privacy, alla protezione dei dati personali e alla conformità alle normative vigenti, quali il GDPR. Infatti, la raccolta, l'elaborazione e la commercializzazione dei dati personali senza un consenso esplicito rappresentano una violazione dei diritti fondamentali degli individui, incluso il diritto alla riservatezza[9].

2. La trasformazione della sfera pubblica e politica come effetto della diffusione della rete

Il fenomeno della mercificazione dei dati personali e la crescente centralità dell'economia digitale hanno effetti che travalicano il solo ambito giuridico ed etico, influenzando in modo significativo anche la sfera pubblica e politica. Il sistema descritto non si limita ad operare per finalità commerciali, ma si estende anche a scopi politici e sociali, soprattutto nel contesto delle piattaforme digitali, dove il controllo dei dati può influenzare opinioni, comportamenti e dinamiche collettive. L'avvento di Internet ha amplificato le tendenze alla disintermediazione e alla privatizzazione della sfera pubblica, adattandole alle caratteristiche distintive del mezzo di diffusione. La rete ha quindi favorito l'emergere di nuove relazioni sociologiche, incastonate nella cornice dello scambio di informazioni tramite apparati tecnologici, inaugurando un sistema di "autocomunicazione di massa"[10]. Questo paradigma sembra soppiantare le modalità comunicative tradizionali, contraddistinte da verticalità e unidirezionalità, con forme di interazione più orizzontali e partecipative[11]. La diffusione di termini come *e-democracy* (democrazia elettronica), *e-government* (governo elettronico) e *e-participation* (partecipazione elettronica) riflettono una crescente aspirazione verso una "comunità" digitale[12]. Internet in passato ha dimostrato il suo valore democratico, come illustrato nella sentenza *Reno v. American Civil Liberties Union* (1997)[13], e ha svolto un ruolo essenziale nella mobilitazione contro regimi autoritari, come dimostrato dai movimenti in Africa settentrionale. Anche altri studi come quelli di M. Margolis e G. Moreno-Riaño[14], esplorano come Internet, grazie alla sua capillarità, possa favorire una democrazia più partecipativa. Risulta infatti particolarmente interessante analizzare come la comunicazione politica si sia evoluta grazie al web. Da un lato la comunicazione politica online rappresenta una rivoluzionaria opportunità di stabilire un contatto diretto e su larga scala con l'elettorato, poiché grazie ai social network i politici possono ora intrattenere un dialogo immediato e continuo con gli elettori, e, nei casi della pubblicazione di contenuti online in maniera organica (esenti quindi dal pagamento di un servizio pubblicitario di diffusione del contenuto offerto dalla piattaforma) si possono superare le barriere economiche precedentemente imposte dalle elevate spese di comunicazione tradizionale (stampa cartacea, televisione, radio, manifesti…). Questa possibilità consente ai rappresentanti politici di veicolare il proprio messaggio in modo più efficiente e capillare, riducendo significativamente i costi associati alla pubblicità e alla propaganda elettorale. Dall'altro lato va sottolineato come i processi democratici stiano subendo, a livello globale, un'erosione di quell'elemento essenziale per la loro vitalità: la sfera pubblica. Il populismo contemporaneo si configura come una nuova e potente macchina da guerra mediatica, capace di trasformare reazioni emotive private in apparenti manifestazioni di opinione pubblica. Siamo immersi in una vera e propria rivoluzione audiovisiva, in cui la mente umana è costantemente *over-stimulated* dai mezzi digitali. Di conseguenza, l'autonomia cognitiva dell'utente non può considerarsi del tutto immune

9. Caso 2021.
10. Castells 2009.
11. Caruso 2023.
12. Longo 2021.
13. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
14. Margolis–Moreno-Riaño 2009.

da potenziali conseguenze preoccupanti[15]. Questo fenomeno è particolarmente insidioso poiché sfrutta la vulnerabilità dei cittadini, ai quali, attraverso tecniche di micro-targeting, vengono somministrate informazioni appositamente costruite per manipolare e strumentalizzare tali fragilità. In tal modo, il dibattito pubblico viene sostituito da una simulazione manipolatoria, che mina le fondamenta stesse della democrazia partecipativa[16]. Le piattaforme online forniscono dunque all'utente una mera illusione di partecipazione in uno spazio pubblico, poiché esse in realtà rinchiudono la persona nel privato delle proprie vulnerabilità ed emozioni[17].

3. Sistemi di raccomandazione, *neural rights* e impatto sulle decisioni

Nel contesto descritto i sistemi di raccomandazione sono diventati onnipresenti su Internet, offrendo agli utenti suggerimenti personalizzati su prodotti e servizi e impattando in maniera significativa sui margini di profitto delle aziende. Ad esempio, Amazon ha riferito che il 35% delle sue vendite proviene dai suoi sistemi di raccomandazione, mentre Netflix nel 2012 ha riportato che il 75% dell'attività di visione dei contenuti derivava da raccomandazioni. I sistemi di raccomandazione influenzano dunque le scelte degli utenti più dei pari e degli esperti, riducendo lo sforzo decisionale[18]. Gli algoritmi sono responsabili di classificare, estrarre, predire, processare dati e così facendo plasmano il mondo in un modo invece che in un altro. Il *ranking* dei contenuti che ci appaiono una volta collegati al nostro *feed* sui social, o nei risultati di un motore di ricerca, non rappresenta solamente una capacità classificatoria ma va a costituire un insieme di strategie all'interno delle quali è insito il potere[19]. Il riferimento, in primo luogo, è all'organizzazione unilaterale dei contenuti proposti sulle piattaforme digitali, che implica una selezione attraverso l'ordine di presentazione, classifiche (*ranking*) e raccomandazioni. Questi processi vengono gestiti dalle stesse piattaforme secondo criteri di rilevanza che tendono a privilegiare determinati contenuti a scapito di altri, basandosi sull'attenzione e sulle emozioni che tali contenuti suscitano. Di conseguenza ciò esercita un primo impatto culturale evidente, poiché le piattaforme digitali, in tale contesto, assumono un ruolo di potere come creatrici di cultura, elaborando unilateralmente i processi di selezione e promozione di ciò che viene discusso o sperimentato sensorialmente (attraverso immagini o suoni) online. In secondo luogo, ci si riferisce anche alla predisposizione unilaterale dei meccanismi di raccolta dei dati cognitivi necessari per tali attività, che si traduce in una gestione altrettanto unilaterale dei processi di catalogazione e, per certi scopi, perfino di denominazione della realtà[20].

Vi sono tuttavia delle restrizioni sulla commerciabilità dei dati che sono frutto delle normative vigenti in materia di protezione dei dati personali, con particolare attenzione alla regolamentazione dei requisiti per il consenso al trattamento, il quale deve essere "libero". Come è noto, tali disposizioni giuridiche bilanciano due interessi contrapposti: da un lato, la promozione della libera circolazione dei dati nel contesto di uno sviluppo del mercato unico dei dati; dall'altro, la salvaguardia dei dati personali, riconosciuta tra i diritti fondamentali nell'ordinamento dell'Unione europea[21].

15. Mancarella 2022.
16. Origgi 2018.
17. Le immagini e i video (spesso generati con tecniche di intelligenza artificiale e diffusi su piattaforme come Facebook, TikTok, Instagram…) che vengono proposti dai politici nelle loro campagne di comunicazione digitali sono infatti sempre più comunemente legati alla volontà di suscitare sentimenti forti, come rabbia, indignazione o paura, piuttosto che persuadere, ovvero ricercare di far cambiare idea a un oppositore.
18. I dati sono stati estrapolati da Nguyen–Hui–Harper et al. 2014. La ricerca non è recente, ma è lecito interpretare questi dati come una indicazione dell'impatto dei sistemi sofisticati di intelligenza artificiale nel produrre ranking di contenuti, che, negli ultimi 10, anni si è accentuato.
19. Garzonio 2021.
20. Orlando 2022-a.
21. Thobani 2019.

Attualmente, il diritto alla privacy include non solo il diritto alla riservatezza, ma anche un più ampio diritto al controllo sui propri dati personali. Si parla ora di *informational privacy*, un concetto ampiamente discusso che riflette la complessità e l'interconnessione della privacy con l'economia dell'informazione. L'*informational privacy* si riferisce alla tutela delle informazioni personali nel quadro delle attività economiche e tecnologiche moderne, dove i dati rappresentano una risorsa fondamentale[22]. Grazie all'intelligenza artificiale, tutti i tipi di dati personali possono essere utilizzati per analizzare, prevedere e influenzare il comportamento umano, trasformandosi così in merci di valore. Informazioni che un tempo non venivano raccolte o erano considerate scarti (i cosiddetti "dati di scarto" o *exhaust data*) sono ora diventate una risorsa preziosa[23].

L'algoritmo costituisce un elemento chiave nell'elaborazione automatizzata dei dati, inclusi quelli destinati a scopi commerciali. Tuttavia, la profilazione[24] tramite algoritmi racchiude in sé una problematica di difficile risoluzione: si configura come uno strumento di marketing vantaggioso sia per le imprese che per i consumatori, ma solleva problematiche relative alla violazione della privacy[25]. S. Rodotà, con riferimento alla navigazione sulla rete Internet e all'uso del social network Facebook, riteneva che solo ed esclusivamente l'anonimato[26] consentisse di "sottrarsi a interferenze nella propria vita che si traducano in aggressioni particolarmente gravi, in discriminazioni, molestie, limitazioni della libertà di espressione, esclusione da circuiti comunicativi"[27].

Infatti, la mancanza di anonimato nell'ecosistema online ha favorito la formazione delle cosiddette *echo chambers*, traducibili come camere d'eco o casse di risonanza, ovvero quegli spazi di navigazione online (come il *feed* di un social network o la homepage) in cui agli utenti vengono mostrati, con regolarità, contenuti simili a quelli con cui hanno già interagito (tramite like, condivisione, click o tempo trascorso in lettura). Un ambiente online personalizzato attraverso il micro-targeting genera bolle di filtraggio[28] o *filter bubbles*, termine coniato da Pariser nel contributo *The filter bubble: What the Internet is hiding from you*, che descrive l'esposizione sistematica degli utenti a informazioni simili per contenuti, con l'effetto di limitare l'incontro con fonti di origine diversa, il che ha per conseguenza l'intensificazione della polarizzazione politica e ideologica. Questo fenomeno è causa di instabilità politica e sociale e aumenta la persuasività di notizie false e teorie complottiste[29]. Una delle esternalizzazioni più preoccupanti di questi fenomeni è rappresentata dalla polarizzazione sociale, che descrive la tendenza a stringere legami solo con persone percepite come simili, escludendo o guardando con sospetto chi è diverso. Un esempio emblematico di questo processo si osserva nel crescente divario tra Democratici e Repubblicani negli Stati Uniti: tra il 1994 e il 2014,

22. Faralli 2019.
23. Lagioia–Sartor 2020.
24. Per una definizione esaustiva di "profilazione" si può far riferimento alla seguente: "la profilazione è una tecnica di trattamento (parzialmente) automatizzato di dati personali e/o non personali, finalizzata alla creazione di conoscenza predittiva mediante la scoperta di correlazioni tra i dati e la costruzione di profili, che possono essere poi utilizzati per assumere decisioni. Un profilo è un insieme di dati correlati che rappresentano un soggetto (individuale o collettivo). La costruzione di profili è il processo di scoperta di schemi ricorrenti e sconosciuti tra i dati, all'interno di grandi insiemi di dati, che possono essere utilizzati per creare profili. L'applicazione di profili consiste nell'identificazione e rappresentazione di uno specifico individuo o gruppo come corrispondente a un determinato profilo, e nel processo decisionale basato su tale identificazione e rappresentazione". Tratto da Bosco–Creemers–Ferraris 2015. Traduzione da Lagioia–Sartor 2020.
25. Bianca 2019.
26. Al tema dell'anonimato online si collega la sentenza Corte europea dei diritti dell'uomo, 7 dicembre 2021, *Standard Verlagsgesellschaft mbH c. Austria* (No. 3), ric. 39378/2015.
27. Rodotà 2012.
28. Pariser 2012.
29. European Data Protection Supervisor, *Online manipulation and personal data*, Opinion 3/2018.

i sentimenti di inimicizia e disapprovazione reciproci sono più che raddoppiati. Questa polarizzazione ostacola la creazione di un capitale sociale che sia inclusivo e capace di "collegare" gruppi diversi, impedendo di fatto una coesione sociale effettiva e costruttiva[30]. In ambito costituzionale, si ritiene che l'evoluzione tecnologica e le trasformazioni nel mercato delle comunicazioni richiedano oggi un approccio diverso per l'analisi del diritto all'informazione, rispetto a quello originariamente previsto dai redattori degli articoli 15 e 21 della Costituzione[31]. Sin dalle sue prime decisioni, la Corte costituzionale ha sempre evidenziato l'importanza fondamentale dell'art. 21, definendolo "pietra angolare dell'ordine democratico" (C. Cost, 17 aprile 1969, n. 84). Partendo da questo principio, la Corte ha affermato che l'art. 21 tutela non solo il "diritto di informare" – ossia l'aspetto attivo della libertà di comunicazione – ma anche il "diritto all'informazione" dei cittadini, essenziale per la corretta formazione dell'opinione pubblica, su cui si basa la democrazia. Il riconoscimento di questo "profilo passivo" della libertà di informazione e il suo legame con il principio democratico implica che tutti i mezzi di comunicazione di massa devono rispondere all'"interesse generale" all'informazione, il quale richiede un pluralismo delle fonti.

Gli studi di Richards[32] aggiungono una nuova chiave di lettura al fenomeno descritto, poiché sottolineano che la consapevolezza di essere costantemente sorvegliati cambia radicalmente il comportamento e le modalità di espressione delle persone, generando un effetto inibitore (*chilling effect*) sulla libertà individuale. In questo contesto, emergono rischi significativi legati alla distorsione comportamentale e alla discriminazione. Le persone il cui comportamento non viene solo influenzato, ma addirittura manipolato attraverso una comunicazione personalizzata, rischiano di diventare diverse da ciò che sarebbero state senza tale manipolazione. La comunicazione mirata sfrutta specifiche vulnerabilità decisionali e comportamentali, alterando profondamente le scelte. Quando si parla di contrastare queste pratiche, ci si riferisce alla necessità di opporsi allo sfruttamento delle vulnerabilità, così come alle pratiche che promuovono la radicalizzazione, la polarizzazione e l'amplificazione di determinati messaggi[33]. Le affermazioni di Richards, se applicate al marketing con finalità politiche, rafforzano l'idea per cui il corretto svolgimento del confronto politico su cui si fonda il sistema democratico (e il tanto discusso diritto all'informazione) stia entrando in una profonda crisi. Viene riconosciuto che la psicografia ha rivoluzionato il marketing degli ultimi anni, permettendo di tracciare un "profilo psicografico" che può essere inferito a partire dai dati di navigazione online di una persona, le tracce che lascia sui social networks, gli acquisti online e i suoi movimenti se usa un telefono cellulare (ad esempio, tramite cookies[34]). Attraverso gli algoritmi e la classica tecnica statistica di analisi di regressione, si riescono a stimare le relazioni tra le differenti variabili, costruendo un profilo psicografico e facendo predizioni sui comportamenti futuri[35]. Queste attività entrano in contrasto con il diritto all'*autodeterminazione informativa*, ovvero al controllo sulla circolazione dei dati riferiti alla singola persona[36]. La "libertà informatica", come descriveva V. Frosini già nel 1981, ha sia un profilo negativo che uno positivo: il primo è "il diritto di non rendere di dominio pubblico certe informazioni di carattere personale", il secondo esprime invece "la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della privacy per essere divenuti

30. S.Calzolaio 2024-a.
31. Donati 2018.
32. Richards 2015.
33. Orlando 2022-b.
34. I cookies sono stringhe di testo che vengono posizionate e archiviate sul dispositivo dell'utente dai siti web visitati (noti come "prime parti" o publisher) o da siti o server web differenti (definiti "terze parti"). Questi cookies vengono poi ritrasmessi ai siti di origine durante le visite successive, permettendo di riconoscere l'utente e memorizzare informazioni utili per migliorare l'esperienza di navigazione.
35. Origgi 2018.
36. Bologna 2021.

elementi di input di un programma elettronico"[37]. Nel volume *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, O'Neill[38] solleva una dura critica per quanto concerne l'affidabilità e l'oggettività solo apparente degli algoritmi. Ella avverte che tali strumenti, spesso frutto di una programmazione superficiale, possono essere portatori di pregiudizi insidiosi e dare origine a previsioni di dubbia veridicità. A tal proposito, emblematica è la menzione del software PredPol, impiegato dalla polizia di Los Angeles per la predizione dei crimini, che ha destato non poche preoccupazioni. Oltre a ciò, O'Neill pone l'accento sul potenziale uso distorto degli algoritmi, come dimostrato dallo scandalo Volkswagen, in cui un software è stato utilizzato per alterare fraudolentemente le rilevazioni delle emissioni inquinanti[39].

Il crescente interesse verso i diritti neurali (e la cosiddetta "identità psichica" presente anche nell'art. 4 del GDPR) può fungere da argine contro l'uso scorretto dei dati personali particolari come quelli neurali, e l'elaborazione di quadri giuridici ed etici che integrino innovazione e diritto di beneficiare del progresso scientifico sono degni di attenzione[40]. Un gruppo di neuroscienziati della Columbia University, guidato dal dottor R. Yuste, ha identificato quattro neurodiritti fondamentali da tutelare: il diritto alla privacy mentale e al consenso, il diritto all'identità personale e al libero arbitrio, il diritto all'accesso equo al potenziamento mentale, e il diritto di tutela dagli errori algoritmici[41]. In questo contesto è utile citare anche il caso del Cile, patria del primo tentativo al mondo di istituire un regime di neurodiritti. La legislazione che ha modificato la costituzione cilena, come sottolineato da Liv e Greenbaum[42], è stata presentata come un passo innovativo verso il riconoscimento di nuovi neurodiritti. Tuttavia, come indicano gli autori, ciò non si è realmente realizzato. I legislatori si sono occupati di introdurre un emendamento costituzionale composto da due parti: la prima, di natura dichiarativa, afferma che i progressi scientifici e tecnologici dovrebbero giovare all'umanità e rispettare il diritto alla vita e all'integrità fisica e mentale; la seconda, di carattere operativo, impone invece una regolamentazione giuridica di tali progressi, con particolare attenzione alla "integrità mentale", intesa come protezione dell'attività cerebrale e delle informazioni da essa derivate. È importante notare come la vera innovazione dell'emendamento costituzionale cileno non risieda tanto nel riconoscimento di un nuovo diritto di "integrità mentale" come neurodiritto in sé, quanto piuttosto nell'istituzione di un nuovo contesto giuridico definito da misure regolatorie.

Nonostante le misure rigorose che le aziende dovrebbero adottare dopo il caso *Cambridge Analytica*[43], non a caso società di produzione di analisi psicografiche, e l'attenzione normativa sui diritti dei soggetti profilati grazie all'entrata in vigore del GDPR, i dati degli utenti che circolano sui social

37. Frosini 1981.
38. O'Neill 2017.
39. Amato Mangiameli 2022.
40. Gulotta–Caponi Beltramo 2021.
41. Yuste–Goering–Agüera y Arcas et al. 2017.
42. Liv–Greenbaum 2024.
43. Chester e Montgomery sintetizzano la vicenda relativa al fenomeno Cambridge Analytica: "In March 2018, The New York Times and The Guardian/Observer broke an explosive story that Cambridge Analytica, a British data firm, had harvested more than 50 million Facebook profiles and used them to engage in psychometric targeting during the 2016 US presidential election. The scandal erupted amid ongoing concerns over Russian use of social media to interfere in the electoral process. The new revelations triggered a spate of congressional hearings and cast a spotlight on the role of digital marketing and 'big data' in elections and campaigns. The controversy also generated greater scrutiny of some of the most problematic tech industry practices – including the role of algorithms on social media platforms in spreading false, hateful, and divisive content, and the use of digital micro-targeting techniques for 'voter suppression' efforts. In the wake of these cascading events, policymakers, journalists, and civil society groups have called for new laws and regulations to ensure transparency and accountability in online political advertising". In Chester–Montgomery 2019.

network restano ancora il "petrolio" ambito anche dai protagonisti dell'agone politico. In particolare, si nota un nuovo interesse, anche a fini politici, per la profilazione dei minori, soprattutto in vista del loro primo voto[44]. Anche per questa ragione, alcuni Paesi hanno iniziato, seppur in modo embrionale, a estendere alcune regole già applicate alla stampa e alla televisione anche ai media digitali, con l'obiettivo di limitare il controllo sui dati da parte delle aziende del settore. Un esempio è dato dalla Spagna e dalla Francia, che hanno deciso di applicare ai media online regole come il silenzio elettorale prima dell'apertura dei seggi, il divieto di diffondere sondaggi o exit poll prima delle elezioni e le limitazioni relative alla pubblicità politica durante le campagne elettorali[45].

4. *Targeting* politico e protezione dei dati personali, tentativi di soluzione europei

Dal punto di vista della privacy, la profilazione presenta implicazioni significative: nel contesto normativo italiano è stata storicamente considerata un'attività di trattamento dei dati particolarmente rischiosa. Inoltre, questa viene concepita come una finalità autonoma, indipendente e specifica, che richiede una base giuridica chiara ed adeguata al fine di essere considerata legittima[46].

In tal senso, l'Unione europea ha avviato diverse iniziative che hanno lo scopo di mitigare le manipolazioni sui processi democratici nel contesto digitale. Una delle prime e più significative è stata l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nel 2018, in cui vengono indicate le basi giuridiche per il trattamento dei dati nella società digitale, volte ad assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche all'interno dell'Unione. Questo regolamento si dimostra anche un elemento chiave nella strategia dell'Ue per la regolamentazione del digitale e aiuta a prevenire e contrastare le pratiche di disinformazione e di manipolazione che si basano sull'uso improprio dei dati personali. Il GDPR mira infatti a rafforzare la protezione e il controllo dei dati personali dei cittadini, sia all'interno dell'Ue che oltre i suoi confini, introducendo diritti che si collegano alla sfera dell'identità online dell'individuo (come il diritto all'oblio, alla cancellazione, alla limitazione e alla rettifica) e procedure per prevenire le violazioni dei dati e limitare gli effetti dannosi della perdita, divulgazione non autorizzata o accesso illecito ai dati[47]. Tra i principi fondamentali della normativa sulla protezione dei dati personali, vi è l'obbligo secondo cui il titolare del trattamento debba sempre identificare una base giuridica adeguata prima di iniziare qualsiasi attività di trattamento dei dati, la quale costituisce la condizione necessaria per la liceità del trattamento stesso. In base alla definizione del Regolamento, l'uso del consenso come base giuridica per il trattamento dei dati dipende strettamente dalla presenza dei requisiti necessari per renderlo valido, ovvero liberamente prestato. Il titolare del trattamento deve quindi verificare che tutti i requisiti previsti dalla normativa siano soddisfatti. In definitiva, è essenziale che il consenso garantisca all'interessato un vero controllo sul trattamento dei propri dati personali e sulle modalità di esecuzione, evitando che tale controllo risulti solo apparente o illusorio[48].

Per ciò che concerne invece le attività elettorali, il GDPR al considerando 56 recita: "Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate". Si nota dunque come la normativa europea abbia riconosciuto in questa sede l'importanza del trattamento dei dati personali da parte dei partiti politici durante le attività elettorali per il buon funzionamento del sistema democratico. In tale contesto, è stato sostenuto che consentire agli attori politici il trattamento dei dati personali a fini di propaganda elettorale costituisca un

44. Ziccardi 2020.
45. Stegher 2023.
46. Banterle 2018.
47. Giacomini 2023.
48. Cassano–Colarocco–Gallus–Micozzi 2018.

"dovere democratico". Tuttavia, è altresì essenziale bilanciare questa esigenza con limiti rigorosi atti a prevenire un utilizzo invasivo e distorto degli strumenti impiegati per tali finalità[49].

L'art. 22 del GDPR, intitolato "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"[50], prevede che, tranne per determinate eccezioni, le decisioni prese in seguito a trattamenti automatizzati di dati personali non possono basarsi su "categorie particolari di dati", ovvero su quelle categorie di dati personali particolarmente sensibili che si ritrovano nell'art. 9 del GDPR, come ad esempio lo stato di salute, il credo religioso, la convinzione politica o l'appartenenza sindacale. Il "diritto alla conoscibilità" dell'algoritmo[51] è strettamente connesso al "diritto di ricevere un'informativa" rispetto al trattamento dei dati effettuato dal titolare, a cui fa riferimento l'art. 13 del medesimo Regolamento Ue[52]. Le linee guida europee sul processo decisionale automatizzato[53], tuttavia, hanno adottato un approccio più prudente nell'interpretare questi riferimenti. Viene infatti riconosciuto che l'interessato ha il diritto di essere informato circa l'esistenza di tali processi decisionali e di ricevere "informazioni significative sulla logica utilizzata", permettendogli così di comprendere la ragione dei trattamenti, specialmente quando le conseguenze potrebbero essere particolarmente rilevanti. Eppure, è importante notare che, nonostante queste indicazioni, non viene esplicitamente menzionato il concetto di *explainability* in modo diretto nel testo normativo[54]. Considerando che i modelli basati sulla monetizzazione dei dati sono ormai una realtà nei mercati dei servizi digitali, la dottrina più attenta si sta interrogando su quale possa essere la base giuridica, ai sensi dell'articolo 6 del GDPR, per legittimare tali trattamenti. In particolare, sono emersi dubbi riguardo alla liceità del trattamento di dati che vanno oltre quelli strettamente necessari per la fornitura del servizio[55]. Un esempio significativo è, come già sottolineato, quello rappresentato dai dati di navigazione degli utenti raccolti dalle piattaforme social, utilizzati per finalità come la pubblicità comportamentale e la personalizzazione dei contenuti[56]. Si rende necessario considerare anche i diritti, strettamente connessi fra loro, alla rettifica e alla cancellazione dei dati, postulati dall'art. 16 e 17 del Regolamento. Ai sensi dell'art. 16, all'interessato spetta il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, nonché

49. Sborlini 2022.

50. L'art. 22 dispone che "l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". La norma non si applica nel caso in cui la decisione automatizzata: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. Nei casi di cui alle lettere a) e c), "il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, a meno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".

51. S.Calzolaio 2017.

52. Mancarella 2022.

53. European Commission 2018.

54. Spiller 2021.

55. Nel contesto descritto è evidente come l'adozione di dati anonimizzati o sintetici (e teoricamente non più personali perché non riconducibili a una persona identificata o identificabile) non sia sempre una soluzione adeguata (si pensi al microtargeting o a studi in ambito medico che incentrano l'attenzione su pazienti specifici). In concreto, se l'uso di dati completamente anonimi o sintetici può ridurre sostanzialmente il rischio di reidentificazione, questa potrebbe non essere una soluzione in tutte le circostanze, poiché in taluni casi, "the truthfulness of the data is lost". Per approfondimenti: Stalla-Bourdillon–Thuermer–Walker et al. 2020,

56. Di Cerbo 2022.

quello di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. Non a caso, il considerando n. 65 del Regolamento tratta congiuntamente il diritto alla rettifica dei dati e quello alla loro cancellazione: entrambi, infatti, sono collegati al diritto individuale alla corretta rappresentazione della "personalità digitale", ovvero alla tutela della cosiddetta "reputazione digitale" (*web reputation*), di cui oggi sempre più frequentemente si invoca la tutela in sede civile e penale[57].

Nel 2018, l'Ue ha inoltre lanciato il *Code of Practice on Disinformation*, un codice di condotta (*soft law*) poi rafforzato nel 2022, sulla disinformazione che si occupa di stabilire una serie di impegni volontari per le piattaforme online aderenti[58]. Tra questi impegni, vi è la promessa di migliorare la trasparenza della pubblicità politica e di prevenire la diffusione di fake news. Riconoscendo l'importanza della pubblicità politica nel plasmare il dibattito pubblico e l'opinione dei cittadini, il codice rafforzato impone ai firmatari di adottare misure di trasparenza più stringenti. Queste misure sono volte a garantire che gli utenti possano identificare chiaramente e facilmente gli annunci politici. In particolare, i firmatari devono implementare un sistema di etichettatura più efficace che evidenzi chiaramente quando un contenuto è un annuncio politico, includendo dettagli essenziali come l'identità dello sponsor, la spesa pubblicitaria sostenuta per l'annuncio e il periodo durante il quale l'annuncio è visibile[59]. Il processo di autoregolamentazione dei social network si colloca all'interno di una strategia promossa dalla Commissione europea, che mira a coinvolgere gli stakeholder nella definizione dei principi e delle direttive necessari per creare una disciplina comune in questo ambito. L'iniziativa punta a lasciare agli stessi social network la responsabilità di implementare le regole più adatte alla loro natura e struttura. Il progetto includeva anche una roadmap per la verifica e l'aggiornamento delle regole adottate dai vari social network coinvolti, garantendo così una continua evoluzione e adeguamento delle normative[60].

La *disinformation* e la *misinformation* sono state inserite tra i rischi sistemici per i processi democratici dall'Ue anche nel Regolamento Ue n. 2065/2022 (*Digital Services Act*), il quale, al considerando 104 statuisce che la disinformazione o le attività di manipolazione e abuso rappresentano rischi sistemici concreti ed effettivi per la democrazia e la società[61]. Il regolamento mira a responsabilizzare maggiormente le piattaforme digitali e a creare un ambiente online più sicuro, richiedendo politiche chiare sui contenuti falsi e manipolati e fornendo maggiore trasparenza sul funzionamento degli algoritmi utilizzati. Il DSA vuole essere uno strumento di aggiornamento e modernizzazione della normativa contenuta nella Direttiva e-commerce, adeguandola agli sviluppi tecnologici e sociali degli ultimi vent'anni, contribuendo a sviluppare condizioni di maggiore sicurezza in rete e riponendo un particolare accento sulle garanzie di tutela degli utenti e sulla protezione della loro libertà di espressione. Per raggiungere questi obiettivi, la Commissione europea ha introdotto obblighi specifici per le grandi piattaforme tecnologiche, note come *big tech*. Queste aziende sono tenute ad assumersi una maggiore responsabilità per quanto riguarda i contenuti illegali o dannosi che vengono diffusi sulle loro piattaforme. L'approccio adottato si basa sulla necessità di bilanciare la libertà di espressione con la protezione degli utenti, cercando di ridurre la diffusione di contenuti nocivi senza limitare ingiustamente la libera circolazione delle idee e delle informazioni[62]. Come descritto, le attività delle piattaforme online infatti non influenzano solo le relazioni economiche e commerciali, ma

57. Allegri 2018.
58. Per porre un argine alla manipolazione dell'informazione sulle piattaforme digitali, il 13 febbraio 2025, la Commissione europea e lo European Board for Digital Services (Comitato Europeo per i Servizi Digitali) hanno approvato l'integrazione ufficiale del Codice di condotta volontario sulla disinformazione nel quadro del *Digital Services Act* (DSA).
59. Commissione europea 2022.
60. Bonini 2020.
61. Ladu–Maccabiani 2023.
62. Flaminio 2022.

rivestono anche un ruolo decisivo nella comunicazione politica e sociale. Non sorprende più che la comunicazione sui social media abbia superato quella dei media televisivi e giornalistici, raggiungendo un pubblico più ampio e diversificato. Il contesto attuale non riguarda solo la sorveglianza dei poteri pubblici sugli individui, ma anche la sorveglianza dei poteri monopolistici privati (*big tech*) nella sfera privata e persino la sorveglianza "alla pari" tra individui, che assumono ruoli reciproci di produttori e consumatori di contenuti all'interno della stessa community[63]. Nello specifico, l'articolo 26 del DSA, intitolato "Pubblicità sulle piattaforme online", estende i diritti degli utenti dei servizi digitali i quali devono essere messi nella condizione di poter identificare chiaramente, in modo conciso e inequivocabile, e in tempo reale, quando un post costituisce una pubblicità. Devono essere informati su ciò che concerne: la persona fisica o giuridica per conto della quale è presentata la pubblicità, chi paga per la pubblicità (se diverso dall'inserzionista) e i parametri utilizzati per determinare a chi viene mostrata la pubblicità, con la possibilità di modificarli quando ciò è applicabile. Analogamente, l'articolo 27, intitolato "Trasparenza dei sistemi di raccomandazione", mira a garantire una maggiore trasparenza per i consumatori, cercando di riequilibrare l'asimmetria informativa nei rapporti *business to consumer* (B2C)[64]. Questo articolo introduce il diritto degli utenti di richiedere la modifica dei criteri di personalizzazione dei contenuti mostrati loro. I gestori delle piattaforme sono obbligati a specificare, in un linguaggio chiaro e comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione e le ragioni per cui vengono suggerite determinate informazioni. Inoltre, gli utenti devono poter accedere a opzioni che permettano loro di modificare tali parametri in qualsiasi momento tramite una sezione dedicata dell'interfaccia della piattaforma, determinando autonomamente a quali informazioni dare priorità[65]. Per inquadrare correttamente da un punto di vista giuridico la tecnologia a monte del funzionamento degli algoritmi, il *machine learning*, ed evitare interpretazioni avventate, come l'idea di una "personalità elettronica", è sufficiente considerare che l'output ottenuto dall'applicazione di un algoritmo (processo) sui dati disponibili (input) non costituisce una regola generale, ma piuttosto un risultato specifico, così come specifico è l'input di partenza. Questo carattere "dal particolare al particolare" permette di classificare questi software di machine learning come procedure di tipo induttivo o inferenziale, e non come sussuntive (dal generale al particolare) o astrattive (dal particolare al generale). In tal senso, il *machine learning* richiama la definizione contenuta nell'art. 2727 del Codice Civile riguardante le presunzioni: "le presunzioni sono le conseguenze che la legge o il giudice trae da un fatto noto per risalire a un fatto ignorato", e, citando O'Neil: "(…) *an algorithm – an opinion formalized in code*"[66].

Il considerando 69 del DSA descrive il caso in cui le inserzioni pubblicitarie vengano presentate ai destinatari attraverso tecniche di targeting mirate ai loro interessi e vulnerabilità, con la possibilità concreta che queste vadano a generare effetti negativi significativi con ripercussioni su interi gruppi, contribuendo ad alimentare campagne di disinformazione e discriminando fasce vulnerabili della popolazione. Le piattaforme online, essendo particolarmente suscettibili a tali dinamiche amplificano i rischi in tal senso. Di conseguenza, i fornitori di queste piattaforme dovrebbero astenersi dall'utilizzare tecniche di profilazione che si basano su categorie particolari di dati personali, come stabilito all'articolo 4, punto 4), e all'articolo 9, paragrafo 1, del GDPR. Il regolamento riconosce che la potenzialità di creare dei danni aumenta rispettivamente all'aumentare delle dimensioni del pubblico di utenti delle piattaforme online. Per mitigare questi rischi, il DSA prevede obblighi aggiuntivi per le piattaforme online molto grandi (quelle con 45 milioni o più di utenti attivi mensili medi nell'Ue). Tra gli obblighi imposti a queste piattaforme si ritrova la necessità di condurre una valutazione annuale dei rischi sistemici significativi causati dai loro servizi e dall'uso che ne viene fatto nell'Unione. Il concetto di "rischi sistemici" si riferisce, tra l'altro, alla diffusione di contenuti

63. Caggiano 2021.

64. Pizzetti–Calzolaio–Iannuzzi et al. 2024.

65. Di Cerbo 2024.

66. Imbruglia 2022.

illegali, alle esternalità negative sui diritti umani e alla manipolazione intenzionale dei loro servizi (articolo 26(1)). Quando vengono identificati rischi sistemici, le piattaforme molto grandi devono adottare misure di mitigazione ragionevoli, proporzionate ed efficaci, come l'adattamento dei loro sistemi di raccomandazione[67]. Si legano al DSA le linee guida rilasciate dalla Commissione e destinate alle piattaforme online e ai motori di ricerca di grandi dimensioni[68], il cui obbiettivo è quello di ridurre i rischi sistemici online che possono influenzare l'integrità dei processi elettorali (è stata prestata una attenzione particolare anche alle passate elezioni del Parlamento europeo dello scorso giugno 2024[69]). Le linee guida suggeriscono misure di mitigazione e pratiche ottimali che le piattaforme e i motori di ricerca di grandi dimensioni dovrebbero adottare prima, durante e dopo gli eventi elettorali.

Sulla base degli sforzi precedentemente descritti, la Commissione europea ha adottato diverse misure per tutelare la libertà e il pluralismo dei media nell'Ue, oltre a promuovere la libera circolazione dei servizi. Questi interventi hanno portato all'approvazione dell'European Media Freedom Act (EMFA), entrato in vigore il 7 maggio 2024. Le nuove norme saranno applicate completamente a partire dall'8 agosto 2025[70]. Per ciò che concerne la presente ricerca, è utile segnalare come il regolamento proponga un meccanismo per evitare che le grandi piattaforme online, come Facebook, X (ex Twitter) o Instagram possano limitare o rimuovere arbitrariamente i contenuti dei media indipendenti. Le piattaforme saranno obbligate a distinguere tra fonti indipendenti e non indipendenti. In caso di intenzione di rimuovere o limitare un contenuto, i media verranno informati e avranno 24 ore per rispondere. Solo dopo la risposta, o in sua assenza, la piattaforma potrà procedere alla rimozione o limitazione del contenuto se questo non rispetta le condizioni della piattaforma. I media potranno inoltre ricorrere a un organo di risoluzione delle controversie extragiudiziale e richiedere un parere dell'European Board for Media Practices (nuovo organo dell'Ue composto da regolatori nazionali, che sarà istituito dal regolamento EMFA)[71]. Accanto a questo regolamento è utile citare anche il *Digital Markets Act* (DMA) che introduce una regolamentazione innovativa e incisiva. Il regolamento intende stabilire una normativa *ex ante* che affianchi e integri la tradizionale disciplina antitrust, con l'obiettivo di promuovere la concorrenza in mercati sempre più dominati dalle *big tech*. In particolare, esso prevede nuovi e stringenti obblighi per le imprese considerate *gatekeeper* (controllori dell'accesso al settore dei servizi e delle piattaforme online), che, grazie alla loro posizione di forza, possono erigere barriere all'ingresso di nuove aziende in mercati come il social networking, il cloud computing e la messaggistica[72].

Risulta interessante citare anche l'esempio dell'ordinamento francese che ha introdotto una normativa specifica per contrastare la manipolazione dell'informazione digitale, soprattutto in relazione all'esercizio dei diritti democratici. Nel dicembre 2018, infatti, è stata promulgata la legge n. 1202, conosciuta come *Loi relative à la lutte contre la manipulation de l'information*. Lo stesso giorno, il 22 dicembre 2018, è stata approvata anche la legge organica n. 1201, composta da soli due articoli, che ha coordinato la normativa con alcune disposizioni di rilevanza costituzionale. La normativa tenta di offrire una regolamentazione complessiva per combattere la disinformazione, sia nell'ambito digitale che nei media tradizionali, soprattutto quando questi ultimi sono influenzati

67. Cauffman–Goanta 2021.
68. Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del Regolamento (UE) 2022/2065. Data di applicazione: 26 aprile 2024.
69. Secondo il *Digital Services Act* (DSA), i servizi con oltre 45 milioni di utenti attivi nell'Ue hanno l'obbligo di affrontare i rischi legati alle elezioni, garantendo al contempo la protezione dei diritti fondamentali, come la libertà di espressione.
70. Vedi la pagina web della Commissione europea *Un nuovo slancio perla democrazia europea*.
71. V. Comunicato stampa del Parlamento europeo.
72. Donati 2021.

da Stati stranieri. L'obiettivo principale è proteggere il sistema democratico francese da manipolazioni esterne che potrebbero destabilizzarlo oltre il normale dibattito politico[73].

In conclusione, nel contesto europeo, il comune patrimonio culturale ha portato i paesi dell'area occidentale, con una tradizione radicata nel costituzionalismo, a sviluppare spontaneamente "principi comuni" all'interno della loro legislazione. La possibilità di un'ulteriore convergenza tra i vari ordinamenti europei sembra strettamente legata alla specificità del contesto europeo, caratterizzato dalla cooperazione multilivello tra istituzioni operanti a livello internazionale, sovranazionale e nazionale. Questa cooperazione si manifesta, da un lato, nella condivisione di istituti giuridici tra le diverse normative nazionali e, dall'altro, attraverso una serie di convenzioni regionali di natura internazionalistica che, in un processo virtuoso, si nutrono delle diverse espressioni di questa tradizione comune, le riflettono, le elaborano e le sintetizzano, reintegrandole successivamente nei singoli ordinamenti nazionali come risultato di esperienze condivise[74].

5. Il regolamento europeo in materia di targeting e trasparenza della pubblicità politica (2024/900)

L'11 marzo 2024 il Consiglio ha adottato un nuovo regolamento europeo relativo alla trasparenza e al targeting della pubblicità politica, volto a contrastare la manipolazione delle informazioni e le ingerenze straniere nelle elezioni. Le nuove norme riguardano la trasparenza e il targeting della pubblicità politica in relazione a un'elezione, a un referendum o a un processo legislativo a livello dell'Ue o in uno Stato membro. Queste non pregiudicano il contenuto dei messaggi di pubblicità politica né altri aspetti relativi alla pubblicità politica, come lo svolgimento di campagne politiche, che rimangono soggette alle norme nazionali specifiche degli Stati membri[75]. In questa sede, l'attenzione sarà posta sulle disposizioni relative alla protezione dei dati personali e ad aspetti di natura costituzionale.

I comma 2 e 3 dell'art.1 del regolamento forniscono interessanti spunti di riflessione, indicando oggetto e obbiettivi del regolamento, occupandosi di escludere "opinioni politiche e altri contenuti editoriali soggetti alla responsabilità editoriale, indipendentemente dal mezzo attraverso cui sono espressi" a patto che non sia previsto un pagamento specifico o altra remunerazione per "la loro preparazione, collocazione, promozione, pubblicazione, consegna o diffusione da parte di terzi o in relazione a tali attività" assieme a "opinioni politiche espresse a titolo personale" le quali "non sono considerate pubblicità politica". Il regolamento dunque non va ad interferire con l'art. 21 della Costituzione italiana, il quale si occupa di garantire la libertà di espressione[76]. Può essere utile ricordare che nel nostro Paese, come descritto da C. Bologna[77], la dottrina dominante sottolinea, alla luce dell'ampia formulazione dell'art. 21 e dell'ispirazione personalista che la permea, il carattere individualistico della libertà di manifestazione del pensiero, anziché un'impostazione funzionalistica. Questo approccio è confermato dall'assenza, nella nostra Costituzione, di disposizioni analoghe all'art. 18 della Legge fondamentale tedesca, che regola l'abuso del diritto orientando l'esercizio della libertà verso il perseguimento di specifici valori politici[78]. Al contrario, la Costituzione italiana adotta un modello pienamente pluralista in materia di libertà di espressione, come dimostrato anche dalla scelta di escludere il limite dell'ordine

73. Fabiano 2023.

74. Borrello 2021.

75. Consiglio Europeo 2024.

76. "Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. […] La stampa non può essere soggetta ad autorizzazioni o censure".

77. Bologna 2021.

78. La legge fondamentale tedesca, come sottolineato da M. Manetti, ripropone a tal fine il concetto di "abuso del diritto" nell'ambito di un ordine ideale di rango costituzionale che non vada solamente a condizionare in maniera esplicita l'esercizio della libertà di pensiero ma che si proponga anche di rifondare il concetto stesso di tale libertà, inserendovi un vincolo che leghi l'individuo alla collettività.

pubblico dal testo dell'art. 21[79]. Si ricorda infatti che lo Stato liberale ha attribuito alla libertà di opinione e di stampa valore costitutivo della sua forma politica, sancendone però al contempo il divieto di "abuso"[80]. Durante il fascismo, pertanto, tale limite era stato interpretato in maniera estensiva, trasformandosi in una clausola suscettibile di essere riempita con i valori dominanti dell'epoca. Di fatto, il regime fascista si è distinto per la tendenza ad estendere il proprio controllo sulle condizioni di esercizio della libertà di stampa, tramite l'istituzione dell'Ordine e dell'Albo dei giornalisti, inteso come meccanismo di filtraggio e accesso "politico" di coloro che avessero voluto esercitare la professione giornalistica, con l'effetto di effettuare un'azione censoria sul contenuto degli stampati[81].

Oggi, la libertà di propaganda, come dichiarato chiaramente dalla Corte costituzionale nella sentenza n. 84 del 1969, è considerata come un'espressione della libertà di manifestazione del pensiero, garantita dall'art. 21 della Costituzione e definita come la pietra angolare dell'ordine democratico. In aggiunta a ciò, le esigenze di tutela del regime democratico, all'interno della Carta costituzionale italiana, possono operare soltanto come un "limite" esterno e non come fondamento di questa libertà, così come delle altre libertà inviolabili[82]. Secondo Spataro[83], sia l'art. 21 della Costituzione che gli artt. 48 e 49 hanno un contenuto difensivo nei confronti di possibili abusi del potere pubblico. Inoltre, questi articoli implicano che il potere pubblico debba compiere interventi positivi finalizzati all'integrazione dei cittadini nella comunità politica statale attraverso una partecipazione reale. Questo approccio mira a evitare "il divorzio tra la titolarità del diritto politico e il suo esercizio". Pertanto, spetta al legislatore garantire le condizioni necessarie per una rappresentanza politica democratica efficace. Risulta utile sottolineare che il ruolo fondamentale attribuito ai partiti dall'art. 49 della Costituzione in questo contesto è centrale: essi sono chiamati a garantire ai cittadini la possibilità di partecipare in maniera democratica alla definizione delle politiche nazionali. Rinunciare a tale funzione significherebbe compromettere il sistema democratico della Repubblica, così come previsto dalla Costituzione. È pertanto compito dei partiti stessi recuperare questo ruolo, che costituisce la loro ragion d'essere: in un contesto dominato dalle tecnologie dell'informazione e della comunicazione (ICT), risulta indispensabile adottare modelli organizzativi che sfruttino queste risorse, senza però trascurare i rischi che esse comportano. Non basta semplicemente impiegare gli strumenti tecnologici, ma è cruciale saperne gestire l'influenza, preservando la propria funzione costituzionale; i partiti devono dunque proporre politiche che non siano limitate alla contingenza del momento o alle emozioni e opinioni del web o delle piazze, ma che riflettano un orizzonte più ampio e lungimirante[84].

Il nuovo regolamento si occupa dunque di distinguere quelli che sono i contenuti organici, ovvero quelli diffusi all'interno di una piattaforma online a titolo personale, senza il pagamento di un servizio di promozione, e quelli sponsorizzati, che vengono mostrati agli utenti a fronte di un compenso versato alla piattaforma. Il regolamento si concentra in particolare sulla pubblicità politica (e non sulla propaganda), definendola all'articolo 3 come "la preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo, di un messaggio fornito normalmente dietro retribuzione o tramite attività interne o nell'ambito di una campagna di pubblicità politica". Tuttavia, la distinzione tra contenuti sponsorizzati e organici può risultare ambigua. Alcuni contenuti, pur non essendo ufficialmente sponsorizzati, riescono a ottenere una vasta diffusione grazie alla viralità, all'uso strategico degli algoritmi e all'abilità di social media manager e *data analyst*

79. Pace–Manetti 2006.

80. Lo Statuto Albertino, all'art. 28 recitava: "La Stampa sarà libera, ma una legge ne reprime gli abusi. Tuttavia le bibbie, i catechismi, i libri liturgici e di preghiere non potranno essere stampati senza il preventivo permesso del Vescovo".

81. Caretti–Cardone 2019.

82. Barbera 1975.

83. Spataro 2022.

84. Morana 2021.

nel massimizzare la visibilità dei messaggi. Questo scenario solleva interrogativi sulla possibilità di aggirare le normative sfruttando meccanismi di amplificazione algoritmica, rendendo più complessa la regolamentazione della pubblicità politica online. Nell'ecosistema della comunicazione politica online, un ruolo significativo è svolto anche dagli influencer, inclusi i micro-influencer, e dagli attivisti, che possono contribuire alla diffusione di determinati messaggi senza che questi rientrino formalmente nella categoria della pubblicità sponsorizzata. Inoltre, le campagne di pubblicità politica possono talvolta fare ricorso a strategie opache o poco trasparenti, come l'uso di reti di social bot, l'attività coordinata di troll, il fenomeno dell'*astroturfing* (ovvero la creazione artificiale di consenso tramite account falsi o organizzazioni fittizie) e l'impiego di *potëmkin personas*, identità digitali costruite ad hoc per influenzare il dibattito pubblico. Questi meccanismi complicano ulteriormente la distinzione tra contenuti organici e sponsorizzati, rendendo più difficile il monitoraggio della trasparenza nella comunicazione politica online. Tale dinamica contribuisce a rendere particolarmente complessa la distinzione tra i messaggi veicolati, i soggetti che li diffondono e coloro che ne sono i reali promotori. Il considerando 30 del regolamento fornisce un segnale che dimostra la consapevolezza dei regolatori del possibile manifestarsi di determinate problematiche: "Un'opinione politica non dovrebbe essere considerata espressa a titolo personale se è prevista una remunerazione specifica da parte di terzi, comprese prestazioni in natura, a fronte dell'espressione di tale opinione o in relazione alla stessa".

Se la libertà di pensiero si compone di due aspetti fondamentali, la formulazione di un'idea e l'utilizzo di un mezzo per la sua diffusione e per la sua acquisizione, è indiscutibile che Internet, per sua stessa natura, offra agli individui enormi possibilità di esprimere e diffondere idee in uno spazio sociale teoricamente più libero e accessibile, in quanto privo di barriere. Tuttavia, è indispensabile sottolineare che la vastissima quantità di informazioni presenti online, prodotta in modo decentralizzato e spesso disorganizzato, richiede un certo ordine per poter essere realmente fruibile dagli utenti[85]. Per questo motivo, sono necessari strumenti che organizzino le notizie sulle pagine web e ne determinino il livello di visibilità, non limitatamente a ciò che concerne i contenuti sponsorizzati.

Il regolamento non estingue del tutto la problematica appena descritta, ma stabilisce in maniera esclusiva: "norme armonizzate sull'uso delle tecniche di targeting e consegna del messaggio pubblicitario che comportano il trattamento di dati personali nel contesto della fornitura di pubblicità politica online" con l'obbiettivo di "tutelare i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla vita privata e la protezione dei dati personali". Viene ravvisata quindi la necessità di intervenire a livello europeo per assicurare una protezione settoriale aggiuntiva ai dati personali trattati per il targeting della pubblicità politica[86], andando oltre, per certi versi, quelle che sono le tutele stabilite dal GDPR. Quest'ultimo prevede già il principio di finalità (contenuto nell'art. 5), il quale comporta il divieto di raccolta e uso di dati personali a fini di targeting elettorale tramite processi di *web crawling*[87]. Su questo tema, il Garante per la protezione dei dati personali è intervenuto più volte, ribadendo gli obblighi normativi che partiti e candidati devono osservare durante le campagne elettorali. In particolare, l'Autorità ha imposto il divieto di utilizzare, per propaganda elettorale e comunicazione politica, dati liberamente accessibili online, inclusi quelli raccolti automaticamente attraverso software specifici o

85. Bazzoni 2019.

86. Il Regolamento offre definizioni per circoscrivere e stabilire il significato di "tecniche di targeting", indicate come "le tecniche usate per rivolgere un messaggio di pubblicità politica solo a una persona specifica o a un gruppo specifico di persone, o per escludere tale persona o gruppo di persone, sulla base del trattamento di dati personali" e le "tecniche di consegna del messaggio pubblicitario", definite come "tecniche di ottimizzazione utilizzate per aumentare la circolazione, la portata o la visibilità di un messaggio di pubblicità politica sulla base del trattamento automatizzato di dati personali e che possono servire a consegnare il messaggio di pubblicità politica a una persona specifica o a un gruppo specifico di persone".

87. Califano 2022.

provenienti da social network, forum o newsgroup, tra cui quelli pubblicati dagli interessati stessi sui social network[88]. La questione relativa al consenso risulta centrale anche nel nuovo regolamento[89]. Il titolare deve infatti ottenere il consenso esplicito e separato per le finalità di targeting e pubblicità politica e tener conto di una garanzia aggiuntiva offerta dal regolamento: "l'obbligo di ottenere il consenso al trattamento dei dati personali non può essere evitato affermando che l'interessato ha reso pubblici i dati personali in questione". A supporto di quanto dichiarato, il considerando 81 include al suo interno un rimando alla "sentenza della Corte di giustizia del 4 luglio 2023 nella causa C-252/21, *Meta Platforms e a.* (Condizioni generali di utilizzo di un social network)", con l'obbiettivo di ribadire la necessarietà di un consenso che sia prestato liberamente e che non vada ad influire sull'accesso ai servizi, e che sia dunque separato dal consenso richiesto per altre finalità al di fuori da quelle per marketing politico[90]. L'obbligo di fornire un'alternativa alla pubblicità politica viene ribadito anche dall'art. 18[91], al comma 4, in cui è stabilito che: "all'interessato che non presta il proprio consenso sia offerta un'alternativa equivalente per l'utilizzo del servizio online senza ricevere pubblicità politica". Un aspetto di particolare rilevanza su cui si è soffermata la Corte di giustizia riguarda la base giuridica utilizzabile per il trattamento dei dati personali ai fini di pubblicità mirate. Generalmente, le piattaforme digitali adottano la posizione secondo cui tale trattamento possa basarsi sull'art. 6, par. 1, lett. f) del Regolamento generale sulla protezione dei dati (GDPR), ossia sul legittimo interesse del titolare del trattamento o di terzi. Tale interpretazione trova un possibile appoggio nel considerando 47 del GDPR, dove si afferma che il trattamento dei dati personali per finalità di marketing diretto possa essere considerato un legittimo interesse[92]. Secondo l'interpretazione del GDPR, il modello "*pay-or-okay*" di Meta non garantisce che il consenso sia prestato liberamente, poiché viene richiesto in un contesto di squilibrio di potere, in modo condizionato, non specifico e dannoso, rendendo il consenso invalido ai sensi dell'articolo 6 del GDPR. Diverse Autorità garanti hanno però riconosciuto la legittimità di questi modelli andando a stabilire ulteriori condizioni specifiche, come la ragionevolezza del prezzo e l'equivalenza delle alternative. Di conseguenza, anche se il modello di Meta potrebbe, con alcune modifiche, essere conforme alle diverse condizioni dei Garanti, non si può sostenere che il consenso degli utenti sia prestato liberamente, il che renderebbe la pratica non conforme al GDPR[93].

Trattando dati personali, segnatamente categorie particolari di dati personali ai sensi dell'art. 9 del regolamento GDPR, è possibile segmentare diversi gruppi elettorali o di privati cittadini e sfruttarne le caratteristiche o vulnerabilità, ad esempio, diffondendo messaggi di pubblicità politica in momenti e luoghi ad hoc per trarre vantaggio da situazioni in cui potrebbe essere più acuta la sensibilità a un certo tipo di informazione/messaggio. Tale trattamento dei dati personali, come segnala il considerando 74 del Regolamento 900, va a generare un impatto negativo sui diritti e sulle libertà fondamentali delle persone, come il diritto di essere trattate in modo equo e paritario, non essere manipolate, ricevere informazioni obiettive, farsi

88. *Provvedimento in materia di propaganda elettorale e comunicazione politica* - 18 aprile 2019.

89. Il consenso al trattamento dei dati personali è dato e revocato in conformità ai regolamenti (UE) 2016/679 e (UE) 2018/1725.

90. "Alla luce della sentenza della Corte di giustizia del 4 luglio 2023 nella causa C-252/21, *Meta Platforms e a.* (Condizioni generali di utilizzo di un social network), gli interessati dovrebbero disporre della libertà di rifiutare, nell'ambito della pubblicità politica, di prestare il loro consenso a operazioni particolari di trattamento di dati, senza essere per questo tenuti a rinunciare integralmente alla fruizione di un servizio online. Come dichiarato dalla Corte di giustizia, a tali utenti dovrebbe essere proposta un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati".

91. L'art. 18 si occupa di stabilire obblighi specifici in materia di tecniche di targeting e di consegna del messaggio pubblicitario in ambito di pubblicità politica online.

92. Battaglia 2023.

93. D'Amico–Pelekis–Santos–Duivenvoorde 2024.

un'opinione, prendere decisioni politiche ed esercitare il diritto di voto. Il considerando prosegue indicando inoltre come queste tecniche vadano ad incidere negativamente sul processo democratico, in quanto conducono a una frammentazione del dibattito pubblico su importanti questioni sociali, a una comunicazione selettiva e, in ultima analisi, alla manipolazione dell'elettorato.

Di particolare interesse è il considerando 79 del nuovo regolamento, perché amplia le garanzie a favore dell'utente rispetto a quanto stabilito dall'art. 9 del GDPR. In concreto, il Regolamento 900, sostiene che nei casi in cui un utente di un social network, nella sua attività di navigazione, visiti una pagina, utilizzi un'applicazione o qualsiasi funzione di un servizio online (per esempio, l'acquisto, per se stesso o terzi di libri a carattere politico, l'utilizzo di applicazioni di preghiera, etc.) a cui si possono riferire una o più categorie di cui all'articolo 9, paragrafo 1 del GDPR, il trattamento di tali dati da parte del gestore dovrebbe essere considerato un trattamento di categorie particolari di dati personali, che è, in linea di principio, vietato (qualora tale trattamento di dati consenta di rivelare informazioni che rientrino in una di tali categorie, anche se tali informazioni non sono necessariamente conformi con l'idea o il pensiero dell'interessato stesso).

Inoltre, si ricorda che l'art. 9 del GDPR prevede alcune eccezioni al divieto di trattare categorie particolari di dati, una delle quali riguarda i dati personali che sono stati resi manifestamente pubblici dall'interessato stesso. Ciò significa, se un interessato rende volontariamente e apertamente accessibili al pubblico alcuni dati sensibili, per esempio attraverso social media o altre piattaforme pubbliche, tali dati potrebbero essere trattati senza che il titolare del trattamento debba rispettare le severe restrizioni normalmente imposte per le categorie particolari di dati personali. Il considerando 80 del nuovo regolamento pone un limite a questa eccezione: "ai fini del presente regolamento, l'obbligo di ottenere il consenso al trattamento dei dati personali non può essere evitato affermando che l'interessato ha reso pubblici i dati personali in questione". Tale limite è in linea con quanto stabilito anche dal DSA e contribuisce alla coscienza di un divieto sempre più diffuso dell'utilizzo di tecniche di *web-crawling* per quanto concerne le categorie di dati particolari.

6. Conclusioni

Nonostante l'ulteriore tutela rispetto a quanto previsto dal GDPR, permangono dubbi sull'efficacia della nuova regolamentazione nel limitare il micro-targeting, poiché essa continua a permettere la profilazione politica e il targeting basati sul consenso dei cittadini (sebbene siano escluse categorie particolari di dati personali ai sensi dell'art.9 del GDPR). Spesso gli utenti non sono pienamente consapevoli dei trattamenti a cui acconsentono, né delle conseguenze che ne derivano. L'affidamento esclusivo al consenso rimane una questione che merita attenzione all'interno del dibattito sul quadro normativo europeo sulla protezione dei dati[94]. L'uso mirato dei dati personali per modellare la percezione politica, spesso senza piena consapevolezza degli utenti, può alterare le dinamiche del dibattito democratico, minando il principio di trasparenza. L'adozione del Regolamento europeo 2024/900 segna dunque un passo in avanti importante per la tutela della privacy e dei diritti fondamentali nell'ambito della pubblicità politica online, introducendo norme specifiche per il trattamento dei dati personali a fini di targeting. Tuttavia, la sua portata limitata ai contenuti di pubblicità a pagamento lascia aperta la questione più ampia dell'influenza algoritmica e della diffusione di contenuti manipolatori esenti dalle più tracciabili sponsorizzazioni tramite piattaforma, i quali non sono direttamente regolamentati. Ciò pone dei dubbi anche presso i cittadini più educati ai media che devono essere messi nelle condizioni di decidere se credere o non credere a quanto viene proposto loro dal sistema di raccomandazione dei contenuti. Questo apre interrogativi su come affrontare strategie di persuasione indiretta, che sfruttano dinamiche virali, reti di influencer e pratiche opache per orientare il dibattito pubblico senza essere direttamente soggette alla normativa. Resta dunque la necessità di un ulteriore approfondimento normativo per affrontare le dinamiche più sottili e pervasive della comunicazione politica digitale, garantendo maggiore trasparenza e protezione agli utenti. Questo vuoto normativo è particolarmente rilevante nel contesto delle campagne di guerra ibrida condotte

94. Ruohonen 2023.

da attori esteri, in primo luogo la Russia, che sfruttano disinformazione e manipolazione algoritmica per polarizzare il dibattito politico, minare la fiducia nelle istituzioni e alterare l'esito dei processi elettorali. La capacità di tali strategie di agire al di fuori dei confini della regolamentazione evidenzia la necessità di un approccio più ampio e coordinato a livello europeo, volto a contrastare le minacce ibride alla democrazia e a garantire un'informazione trasparente e pluralista. Per far fronte a tali minacce, alcune nazioni europee hanno istituito delle agenzie nazionali volte alla salvaguardia psicologica dei cittadini, come in Svezia l'Agenzia per la difesa psicologica, attiva dal 2022 e operante sotto il Ministero della Difesa, costituita da un team specializzato nella lotta alla disinformazione e nell'analisi digitale. Anche la Francia ha attivato il Servizio di vigilanza e protezione contro le ingerenze digitali estere (Viginum), istituito nel 2021 sotto il Segretariato generale della difesa e della sicurezza nazionale del Primo Ministro la cui *mission* principale è individuare e analizzare le ingerenze digitali straniere che influenzano il dibattito pubblico online in Francia. Attualmente, in Italia, il DDL 1090 del 2024 per "l'istituzione dell'Agenzia sulla disinformazione e la sicurezza cognitiva" (ADISC) rimane solamente una proposta.

A partire dalla fine del 2025, con l'applicazione del nuovo regolamento, sarà possibile valutarne l'impatto sull'ecosistema digitale. Google ha già annunciato l'eliminazione *in toto* della pubblicità politica, mentre Meta non ha ancora definito una posizione. Se anche altre piattaforme seguissero questa linea, si rischierebbe di ridurre ulteriormente lo spazio per il dibattito politico online, con effetti potenzialmente contrari a quelli auspicati dalla normativa. Se da un lato la regolamentazione limita la pubblicità politica, dall'altro emergono nuove modalità di infiltrazione nel dibattito pubblico, come l'uso di troll, bot e strategie coordinate per influenzare l'opinione pubblica senza ricorrere alla pubblicità tramite adv e sponsorizzazioni. La campagna elettorale è un momento fondamentale per le democrazie, poiché consente di proporre idee e candidati, alimentando il confronto politico. Tuttavia, le nuove restrizioni e i cambiamenti nel panorama digitale pongono interrogativi su quali strumenti rimarranno disponibili per la comunicazione politica e in che misura questi cambiamenti influenzeranno la trasparenza e il pluralismo del dibattito pubblico.

Riferimenti bibliografici

M.R. Allegri (2018), *Diritto all'oblio, tutela della* web reputation *individuale e "eccezione giornalistica". Spunti giurisprudenziali*, in "Forum di Quaderni Costituzionali - Rassegna", 11 giugno 2018

A.C. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

F. Banterle (2018), *Pubblicità comportamentale, GDPR e rischi di discriminazione*, in S. Bonavita (ed.), "Società delle tecnologie esponenziali e General Data Protection Regulation", Ledizioni, 2018

A. Barbera (1975), *Art. 2*, in G. Branca (ed.), "Commentario della Costituzione", Zanichelli, 1975

F. Battaglia (2023), *La sentenza Meta platforms. Riflessioni in materia di valore dei dati e libera espressione del consenso*, in "Ordine internazionale e diritti umani – Osservatorio sulla Corte di Giustizia dell'Unione europea", 2023, n. 3

G. Bazzoni (2019), *La libertà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei* global social media, in "Diritto di Internet", 2019, n. 4

M.R. Bianca (2019), *La* filter bubble *e il problema dell'identità digitale*, in "MediaLaws", 2019, n. 2

N. Bobbio (1990), *L'età dei diritti,* Einaudi, 1990

C. Bologna (2021), *Libertà di espressione e riservatezza «nella rete»? Alcune osservazioni sul mercato delle idee nell'*agorà *digitale*, in "Gruppo di Pisa", Quaderno n° 3, fascicolo speciale monografico abbinato al n. 2/2021

P. Bonini (2020), *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in "federalismi.it", 2020, n. 11

R. Borrello (2021), *Le forme di raccordo tra le autorità indipendenti nazionali e la realizzazione di un modello comune europeo di disciplina della comunicazione politica: recenti sviluppi*, in "DPCE Online", vol. 47, 2021, n. 2

F. Bosco, N. Creemers, V. Ferraris et al. (2015), *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth, R. Leenes, P. de Hert (eds.), "Reforming European Data Protection Law", Springer, 2015

G. Caggiano (2021), *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in "Annali AISDUE", 2021, n. 1

L. Califano (2022), *Comunicazione politica e social network*, in "Cultura giuridica e diritto vivente", vol. 10, 2022

L. Califano (2021), *Come si governa la tecnologia digitale?*, in "Cultura giuridica e diritto vivente", vol. 8, 2021

E. Calzolaio (2023), *Beni digitali e proprietà tra* civil law *e* common law, in "Rivista critica del diritto privato", 2023, n. 3

S. Calzolaio (2024-a), *Isolamento e relazioni sociali. Il Connection-in-All-Policies approach. Nota a: U.S. Surgeon General, Our epidemic of loneliness and isolation: The U.S. Surgeon General's advisory on the healing effects of social connection and community, 2023*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2024-b), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2018), *Recensione di N. Richards, Intellectual privacy. Rethinking civil liberties in the digital age. New York, NY: Oxford University Press, 2017, pp. 220*, in "Giornale di storia costituzionale", 2018, n. 36

S. Calzolaio (2017), *Protezione dei dati personali*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), "Digesto delle Discipline Pubblicistiche", Aggiornamento, 2017

P. Caretti, A. Cardone (2019), *Diritto dell'informazione e della comunicazione nell'era della convergenza tecnologica*, il Mulino, 2019

C. Caruso (2023), *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in "Quaderni costituzionali", 2023, n. 3

R. Caso (2021), *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Ledizioni, 2021

G. Cassano, V. Colarocco, G.B. Gallus, F.P. Micozzi (a cura di) (2018), *Il processo di adeguamento al GDPR*, Giuffrè, 2018

M. Castells (2009), *Comunicazione e potere*, Università Bocconi Editore, 2009

C. Cauffman, C. Goanta (2021), *A new order: The Digital Services Act and consumer protection*, in "European Journal of Risk Regulation", vol. 12, 2021, n. 4

J. Chester, K.C. Montgomery (2019), *The digital commercialisation of US politics – 2020 and beyond*, in "Internet Policy Review", December 2019

Commissione europea (2022), *Codice di buone pratiche sulla disinformazione 2022*

Consiglio Europeo (2024), *L'UE introduce nuove norme in materia di trasparenza e targeting della pubblicità politica*, comunicato stampa, 11 marzo 2024

V. Cuffaro (2019), *Il diritto europeo sul trattamento dei dati e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

A.S. D'Amico, D. Pelekis, C. Santos, B. Duivenvoorde (2024), *Meta's pay-or-okay model: An analysis under EU data protection, consumer, and competition law*, Utrecht University School of Law Research Paper 1-2024

A. Di Cerbo (2024), *La tutela dell'identità nell'ambiente digitale alla luce delle norme europee*, in "European Journal of Privacy Law & Technologies", 2022, n. 2

A. Di Cerbo (2022), *L'inquadramento giuridico dei dati personali ceduti per la fruizione dei servizi digitali*, in "European Journal of Privacy Law & Technologies", 2022, n. 2

F. Donati (2021), *Verso una nuova regolazione delle piattaforme digitali*, in "Rivista di regolazione dei mercati", 2021, n. 2

F. Donati (2018), *L'art. 21 della Costituzione settanta anni dopo*, in "MediaLaws", 2018, n. 1

G. Donna (2018), *Modello di business, patrimonio strategico e creazione di valore*, in "Impresa Progetto. Electronic Journal of Management", 2018, n. 2

European Commission (2018), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 22 August 2018

L. Fabiano (2023), *Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati*, in "Il Diritto dell'informazione e dell'informatica", 2023, n. 4-5

C. Faralli (2019), *La privacy dalle origini ad oggi. Profili storico-filosofici*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam 2019

S. Flaminio (2022), *Lotta alle fake news: Dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act*, in "Rivista italiana di informatica e diritto", 2022, n. 2

V. Frosini (1981), *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), "Privacy e banche dati", il Mulino, 1981

Garante per la protezione dei dati personali (2019), *Provvedimento in materia di propaganda elettorale e comunicazione politica - 18 aprile 2019*

E. Garzonio (2021), *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in "Rivista italiana di informatica e diritto", 2021, n. 2

A. Genus, A. Stirling (2018), *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, in "Research Policy", vol. 47, 2018, n. 1

G. Giacomini (2023), *Il GDPR e la regolamentazione della sfera digitale. Orientamenti degli italiani circa la disinformazione su Internet*, in "Comunicazione politica", 2023, n. 3

S. Gobbato (2019), *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in "MediaLaws", 2019, n. 3

G. Gulotta, M. Caponi Beltramo (2021), *Neurodiritti: tra tutela e responsabilità*, in "Sistema Penale", 1 ottobre 2021

W. Hartzog, N.M. Richards (2022), *The Surprising Virtues of Data Loyalty*, in "Emory Law Journal", vol. 71, 2022, n. 5

D. Kerpen (2011), *Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Generally Amazing on Facebook (And Other Social Networks)*, McGraw-Hill, 2011

D. Imbruglia (2022), *Diritti fondamentali e ambienti digitali: prime note di una ricerca sul diritto a non essere sottoposto a una decisione interamente automatizzata*, in S. Orlando, G. Capaldo (a cura di), "Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università editrice, 2022

N. Irti (2019), *Il tessitore di Goethe (per la decisione robotica)*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

M. Ladu, N. Maccabiani (2023), *L'autodeterminazione popolare nell'era digitale: tra opportunità normative e tecnologiche*, in "Consulta Online", 2023, n. 2

F. Lagioia, G. Sartor (2020), *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in "federalismi.it", 2020, n. 11

N. Liv, D. Greenbaum (2024), *Integrating Mental Privacy within Data Protection Laws: Addressing the Complexities of Neurotechnology and the Interdependence of Human Rights*, in "AJOB Neuroscience", vol. 15, 2024, n. 2

E. Longo (2021), *Rivoluzione digitale e sviluppi della partecipazione democratica nell'Unione europea*, in "Osservatorio sulle fonti", 2021, n. 3

M. Mancarella (2022), *Social media e comunicazione politica: quali rischi per il sistema democratico?*, in "Rivista elettronica di Diritto, Economia, Management", 2022, n. 3

M. Margolis, G. Moreno-Riaño (2009), *The Prospect of Internet Democracy*, Routledge, 2009

U.A. Mejias, N. Couldry (2019), *Datafication*, in "Internet Policy Review", vol. 8, 2019, n. 4

A. Morace Pinelli (2024), *Introduzione*, in Id. (a cura di), "Dalla *Data Protection* alla *Data Governance*: il regolamento (UE) 2022/868. Commentario al *Data Governance Act*", Pacini Giuridica, 2024

D. Morana (2021), *Partiti e partecipazione politica nell'era digitale: la prospettiva costituzionale*, in "Rivista trimestrale di diritto pubblico", 2021, n. 2

T.T. Nguyen, P.M. Hui, F.M. Harper et al. (2014), *Exploring the filter bubble: The effect of using recommender systems on content diversity*, in "WWW '14: Proceedings of the 23rd International Conference on World Wide Web", Association for Computing Machinery, 2014

C. O'Neill (2017), *Armi di distruzione matematica: come i big data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, 2017

G. Origgi (2018), *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in "Ragion pratica", 2018, n. 51

S. Orlando (2022-a), *Data vs capta: intorno alla definizione di dati*, in "Nuovo diritto civile", 2022, n. 4

S. Orlando (2022-b), *Per un sindacato di liceità del consenso privacy*, in "Persona e Mercato", 2022, n. 4

A. Pace, M. Manetti (2006), *Rapporti civili. Art. 21. La libertà di manifestazione del proprio pensiero*, Zanichelli, 2006

E. Pariser (2012), *The Filter Bubble: What the Internet is Hiding from You*, Penguin, 2012

F. Paruzzo (2022), *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Edizioni Scientifiche Italiane, 2022

F. Pizzetti, S. Calzolaio, A. Iannuzzi et al. (2024), *La regolazione europea della società digitale*, Giappichelli, 2024

N.M. Richards (2015), *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford University Press, 2015

S. Rodotà (2012), *Il diritto di avere diritti*, Laterza, 2012

J. Ruohonen (2023), *A Note on the Proposed Law for Improving the Transparency of Political Advertising in the European Union*, 2023

D. Sborlini (2022), *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 6

O. Spataro (2022), *Diritti di partecipazione politica e piattaforme digitali, alcune riflessioni*, in "Dirittifondamentali.it", 2022, n. 2

E. Spiller (2021), *Il diritto di comprendere, il dovere di spiegare.* Explainability *e intelligenza artificiale costituzionalmente orientata*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 2

S. Stalla-Bourdillon, A. Knight (2017), *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in "Wisconsin International Law Journal", vol. 34, 2017

S. Stalla-Bourdillon, G. Thuermer, J. Walker et al. (2020), *Data protection by design: Building the foundations of trustworthy data sharing*, in "Data & Policy", 2020, n. 2

G. Stegher (2023), *Da cittadini elettori a cittadini consumatori: osservazioni sull'importanza di regolare le campagne elettorali sui social media*, in "Nomos", 2023, n. 1

I. Stepanov (2019), *Introducing a property right over data in the EU: the data producer's right – an evaluation*, in "International Review of Law, Computers & Technology", vol. 34, 2019, n. 1

C.R. Sunstein (2006), *Infotopia: How Many Minds Produce Knowledge*, Oxford University Press, 2006

S. Thobani (2019), *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in "MediaLaws", 2019, n. 3

R. Yuste, S. Goering, B. Agüera y Arcas et al. (2017), *Four ethical priorities for neurotechnologies and AI*, in "Nature", vol. 551, 2017

H. Zech (2016), *Data as a tradeable commodity*, in A. De Franceschi (ed.), "European contract law and the digital single market: Implications of the digital revolution", Intersentia, 2016

G. Ziccardi (2020), L'*uso dei social network in politica tra alterazione degli equilibri democratici, disinformazione, propaganda e dittatura dell'algoritmo: alcune considerazioni informatico-giuridiche*, in "Ragion pratica", 2020, n. 54

S. Zuboff (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019

F. Zuiderveen Borgesius, D. Trilling, J. Möller et al. (2016), *Should we worry about filter bubbles?*, in "Internet Policy Review", vol. 5, 2016, n. 1

Studi e ricerche

Sistemi e applicazioni

Note e discussioni

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0207 • articolo sottoposto a peer review • pubblicato in anteprima il 18 feb. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Maria Chiara Pollicino

Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa

Il saggio analizza l'interazione tra il nuovo Regolamento sulle intelligenze artificiali e il GDPR al fine di valutare il complessivo impatto, frutto della sommatoria tra le due citate normative, nell'ambito dell'attività amministrativa. L'integrazione tra le due discipline risulta inevitabile, soprattutto sul piano fenomenologico, poiché l'impiego dell'intelligenza artificiale implica quasi sempre il trattamento di dati personali. A tal fine, anche per esigenze di chiarezza espositiva, i due testi saranno analizzati prima separatamente, ponendo in evidenza le peculiarità che assumono allorquando il trattamento dei dati personali o l'uso dell'intelligenza artificiale abbia luogo nella cornice dell'azione pubblica. All'esito della trattazione separata, i due Regolamenti saranno posti a confronto, evidenziandone i principali elementi comuni e differenziali. In ultimo, alla luce del confronto, si ragionerà sull'impatto della complessiva normativa sul potere pubblico.

Privacy – Pubblica amministrazione – Intelligenza artificiale – GDPR – AI Act

The effects of the "cumulative impact" of the GDPR and the new Artificial Intelligence Regulation in the context of administrative activities

This paper draws a comprehensive interaction between the new Artificial Intelligence Regulation and the GDPR, with the goal of assessing their combined impact on administrative activities. The intersection of these two frameworks is, in most cases, inevitable, particularly on a phenomenological level, as the use of artificial intelligence involves the processing of personal data. To achieve this, the two regulations will first be examined individually, emphasizing the unique characteristics each assumes when personal data processing or the use of AI occurs within the realm of public administration. Following this individual analysis, the regulations will be compared, highlighting their key similarities and differences. Finally, based on the insights from this comparison, the overall effect of these regulatory frameworks on the exercise of public authority will be carefully evaluated.

Privacy – Public Administration – Artificial Intelligence – GDPR – AI Act

L'Autrice è dottoranda in Legalità, culture politiche e democrazia, profilo di diritto amministrativo, presso l'Università degli Studi di Perugia

Sommario: 1. Premessa: l'impatto della regolazione nel settore digitale. Perché regolare e quanto regolare? – 2. Le peculiarità del trattamento dei dati da parte dei soggetti pubblici. Una ricognizione delle norme più rilevanti del GDPR in materia. – 2.1. La base di liceità di cui all'art. 6, par. 1, lett. e). – 3. Il Regolamento sulle intelligenze artificiali: la filosofia di fondo. – 3.1. Le norme del Regolamento IA più rilevanti per l'attività pubblicistica. – 4. Il Regolamento IA e GDPR a confronto: analogie e differenze tra le due fonti. – 4.1. Ancora sul rapporto GDPR e Regolamento IA. La DPIA *versus* la FRIA: la duplicazione di adempimenti per le amministrazioni. – 5. Osservazioni conclusive: le problematiche sottese all'applicazione congiunta dei due regolamenti. Il rischio di eccesso di regolazione della tecnologia per il settore pubblico.

1. Premessa: l'impatto della regolazione nel settore digitale. Perché regolare e quanto regolare?

Prima di entrare nel merito della questione circa l'attuale quadro regolatorio del digitale e, in particolare, valutare le eventuali sovrapposizioni tra il GDPR e il nuovo regolamento sulle intelligenze artificiali[1] sotto la lente del trattamento effettuato dal soggetto pubblico, è opportuno riflettere sul perché rispondere alla domanda relativa a quale sia l'ottimo regolatorio del settore digitale nel pubblico sia diventato fondamentale[2]. Difatti, regolare adeguatamente il settore del digitale ha un immediato impatto, oltre che sui principi del procedimento amministrativo, come il principio di legalità o la trasparenza, sui diritti fondamentali dell'uomo[3] e, ancor più a monte, sulla tenuta democratica degli Stati[4].

Molti studiosi oltreoceano hanno, già da tempo, evidenziato l'impatto sociale di scelte regolatorie "errate" sulle tecnologie[5]: regolare poco o, al contrario, regolare troppo le tecnologie potrebbe avere delle conseguenze significative su larga scala, soprattutto se si considera il settore pubblico.

Regolare "poco", difatti, renderebbe possibile il concretizzarsi di tutta una serie di pericoli: tra cui la nascita di nuove forme di discriminazione nonché, a monte, un importante sbilanciamento dei rapporti di forza tra i poteri pubblici e privati, a favore dei secondi.

Sotto il primo profilo richiamato, la discriminazione che si potrebbe creare, per esempio, delegando decisioni alla macchine – in modo più o meno consapevole – senza un'adeguata normativa a sostegno che possa neutralizzare i pericoli di *bias*[6]. Più nello specifico, è stato evidenziato che

1. Regolamento (UE) 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale, di seguito detto, in breve Regolamento IA.
2. Tale domanda, sull'ottimo regolatorio, diviene ancor più interessante considerando che l'Europa si è ritagliata una funzione di *leadership* nella regolazione nel settore a livello globale. Tale ruolo trova conferma negli scritti della dottrina mondiale, *ex multis*, citando autori statunitensi, cfr. Solove–Schwarts 2022.
3. Niro 2021; Simoncini–Suweis 2019; Calzolaio 2023; Iannuzzi 2021.
4. Barocas–Selbst 2016.
5. *Ibidem*.
6. Proprio per disinnescare tale possibilità si richiede che ogni decisione algoritmica sia assistita dal controllo umano. Tuttavia, spesso, tale previsione, se non adeguatamente declinata, rischia di tradursi in un controllo formale e non sostanziale da parte dell'umano. Sul punto, si rimanda a quanto evidenziato da Carloni

potrebbero perpetrarsi fenomeni come quello della c.d. "discriminazione istituzionalizzata"[7] fondata, per l'appunto, su *bias*, ossia pregiudizi inconsci delle macchine e, poi, fatti propri dai decisori pubblici (peraltro, si tratta di errori che, per loro natura, sono destinati a ripetersi *n* volte). Uno dei problemi maggiori che pongono simili *bias* involontari – in quanto non diretto frutto di una opera dei programmatori che hanno tarato male la macchina – è che gli stessi, di sovente, sono irriconoscibili dall'uomo[8]: in questo senso, l'ingiustizia umana volontaria è un fenomeno molto più auto-evidente comparata all'ingiustizia involontaria algoritmica[9].

Per quanto concerne il secondo profilo citato, il potere privato, ad oggi, tramite la tecnologia, ha assunto una peculiare forza non solo economica[10], bensì, anche negli ambiti, tradizionalmente "riservati" al potere pubblico, sociale e politico. Come evidenziato da attenta dottrina: «non vi è dubbio (…) che i grandi fornitori di servizi digitali siano ormai poteri privati globali di grandi dimensioni, dotati di un enorme peso economico e di presenza e influenza molto pervasive sul piano sociale»[11]. Pertanto, ad oggi, la necessità di una regolazione adeguata si impone in quanto il potere pubblico è chiamato non solo a porre delle norme di contenimento del settore privato, che sfugge al controllo del pubblico, bensì si tratta di normare il settore privato – in una vera e propria lotta per la sovranità[12] – con il pubblico[13]. È stato osservato che uno dei vantaggi del potere privato rispetto al potere pubblico consiste nel fatto che è difficile regolare *ex ante* un qualcosa che non si conosce e che si sviluppa fuori dal contesto istituzionale. La tecnologia, difatti, tendenzialmente, non si sviluppa all'interno

2020, p. 281: «(i)n assenza di una disciplina legislativa ad hoc, ed in ogni caso per riflettere sui limiti e le condizioni che potrebbero accompagnare una simile regolazione, è altrove che bisogna guardare per ragionare sulla possibilità e legittimità di una decisione algoritmica, intendendo con questa una decisione non elementare assunta sulla base di un percorso decisionale non meramente meccanico ma rimesso a macchine. Dove si intende per "rimesso" il fatto che la decisione sia effettivamente adottata in assenza di un intervento umano nella fase decisionale, ma anche già solo il fatto che l'operazione automatizzata effettuata svolga un ruolo decisivo nella determinazione provvedimentale e non sia in sé suscettibile di revisione, quanto alla correttezza intrinseca del "ragionamento" seguito, da parte del funzionario istruttore».

7. Il termine è stato coniato in ambito sociologico da Pager–Shepherd 2008.
8. Cfr. anche Powell 2007.
9. Barocas–Selbst 2016, p. 674 ove si evidenzia: «(…) Because the discrimination at issue is unintentional, even honest attempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions. Furthermore, because the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address». Ancora, parte della dottrina ha sottolineato come, a monte, regolare il fenomeno tecnologico sia una sfida molto complessa per il diritto, che rischia di perdere il suo ruolo di "strumento di regolazione dei conflitti umani" cfr. Corasaniti 2022, pp. 11-12: «Il diritto rischia di non adeguarsi al passaggio, di non potere mantenere a lungo il suo tradizionale ruolo di strumento di regolazione dei conflitti umani non riuscendo a comprendere né a definire in modo tradizionale ambiti e forme di regolazione, tanto più se questi debbono svolgersi in un contesto senza confini in uno spazio cyber definito e ricompreso nelle piattaforme di servizio nelle quali i soggetti si collocano, peraltro liberamente. Le piattaforme digitali oggi operano in assoluta interconnessione e condizionano e condizioneranno sempre di più le scelte dei soggetti sociali, indirizzandole, uniformandole, facilitandole e trasformandole in un progetto di vita o di attività vitale».
10. Per dare un'idea della forza economica dei colossi del digitale, si pensi che, tra le società quotate nella borsa di Wall Street, Apple è la prima società ad avere toccato il valore di tremila miliardi di dollari. Come ben evidenziato da Torchia 2024.
11. *Ivi*, p. 18.
12. Sulla battaglia pubblico-privato si vedano: Betzu 2021.
13. Cfr. Torchia 2024.

del settore pubblico, al contrario, «si sviluppa fuori dalle grandi istituzioni di ricerca»[14].

In ogni caso, la capacità del potere privato di influenzare la società[15] è ancor più preoccupante considerando che le nuove tecnologie permettono alle intelligenze artificiali di "entrare" in aspetti profondamente intimi dell'essere umano tra cui il pensiero (ci si riferisce al tema, delicatissimo, della privacy mentale)[16].

Queste, dunque, le principali problematiche che deriverebbero da una regolazione assente, scarna o, comunque, inefficace.

Per converso, all'opposto, regolare "troppo" vorrebbe dire, nella sostanza, rendere quasi impossibile un utilizzo proficuo degli strumenti tecnologici che, invece, possono costituire un validissimo strumento per l'attività pubblica, andando ad attuare i principi di buon andamento e di efficienza previsti, in primo luogo, dalla Costituzione, all'art. 97[17].

Perché regolare troppo rende quasi impossibile l'utilizzo delle tecnologie? Sul punto, occorre svolgere una sintetica premessa. Di sovente, quando si parla di amministrazione o di esercizio delle funzioni pubbliche, si dimentica di considerare il fattore umano: ossia, sono i singoli funzionari, che portano avanti il procedimento amministrativo e, in generale, l'azione pubblica, a dover applicare, *de facto*, quella o quell'altra norma e, a monte, a scegliere *come gestire il procedimento* (naturalmente negli spazi concessi dalla legge[18]).

Orbene, proprio considerando tale fattore umano, l'eccesso di regolazione può portare alla non trascurabile difficoltà per il funzionario[19] di inquadrare correttamente la normativa applicabile alle singole fattispecie e, pertanto, si potrebbe preferire di rifuggire l'uso di tecnologie avanzate; in altri termini, se il quadro giuridico non è facilmente accessibile perché vi è una ipertrofia normativa, il funzionario pubblico[20] potrebbe essere portato: *i)* o ad allungare i tempi del procedimento che si avvale di tecnologie all'avanguardia al precipuo fine di scioglierne i dubbi giuridici (per esempio,

14. *Ivi*, p. 16 la quale evidenzia: «viene sempre citato in proposito il famoso garage in cui Bill Gates, dropout dell'Università di Harvard, diede i natali a Microsoft – ma anche grazie a esse: basti ricordare che Internet nasce come Arpanet, alla fine degli anni Sessanta, grazie al centro militare Arpa e ad alcune università della California».
15. Il tema dell'affermarsi dei poteri privati in ambiti tradizionalmente riservati ai poteri pubblici ha un immediato riflesso sulla tenuta democratica degli Stati, come evidenziato dalla dottrina in materia di moderazione dei post per il mezzo di comitati di controllo gestiti dagli stessi social networks: cfr. Pollicino 2019, p. 10 ss.
16. D'Avack 2023 a p. 1710 e ss.: «(l)e potenzialità di penetrazione della tecnica – nell'ambito della interazione tra IA e neuroscienze e neurotecnologie – nella sfera più intima del soggetto, quella del pensiero e dei suoi correlati neuronali, solleva interrogativi di natura etica e giuridica su come proteggere questi dati così sensibili, anche dai rischi di una circolazione potenzialmente discriminante; sui confini e sulle implicazioni della libertà psichica e cognitiva di un soggetto, della sua "integrità" mentale, sulla possibilità – che deve essere sempre garantita – di disconnettersi dal mezzo di interfacciamento».
17. Sulla connessione art. 97 Cost. e uso delle intelligenze artificiali si veda Cerrina Feroni 2023: «Da qui il problema se sottoporre la persona alla decisione integralmente automatizzata di un software risulti in sé lesivo della dignità della persona stessa. Non si tratta di assumere posizioni di contrarietà agli sviluppi tecnologici, forieri sicuramente del migliore perseguimento di interessi pubblici e, quindi, funzionali al buon andamento della p.a. di cui all'art. 97 Cost. Ma di porre in evidenza, già partendo dal quadro costituzionale, che la tutela della dignità della persona richiede che l'intervento dell'uomo nel compimento della scelta amministrativa non sia del tutto obliterato o marginalizzato, proprio per rispettare la gerarchia assiologica voluta dalla Costituzione e alzare un argine alla "disumanizzazione" dell'amministrazione, riportando la macchina a semplice strumento dell'azione amministrativa».
18. Sul punto, si rimanda alle innumerevoli trattazioni scientifiche sul tema legalità/discrezionalità amministrativa, *ex multis*: Police 2014.
19. Si parla di funzionario in termini non tecnici intendendosi, in tal senso, un qualsiasi dipendente pubblico chiamato a esercitare un certo potere nel concreto, sia lo stesso funzionario, dirigente etc.
20. Potrebbe essere non del tutto accessibile o alla luce di una normativa oscura o perché vi sono troppe fonti che regolano quella specifica attività.

acquisendo pareri e così via), così ponendo nel nulla uno dei vantaggi maggiori della tecnologia, ossia la velocità *ii)* o, ancor peggio, ad evitare in radice l'utilizzo di tecnologie avanzate nel timore di errori giuridici tali da concretizzare ipotesi di violazioni normative, con conseguente rischio di responsabilità amministrativa. Sul punto, è opportuno menzionare una recente pronuncia, emessa nel 2024, dalla Corte dei conti che riconosce una responsabilità erariale del *Data protection Officer*[21].

Non è un mistero, difatti, che uno dei problemi più dilaganti nell'ambito dell'amministrazione italiana è stata (ed è) la c.d. paura della firma[22]; similmente al fenomeno della paura della firma, regolare troppo, potrebbe condurre l'operatore pubblico a evitare l'utilizzo delle tecnologie più avanzate alla luce della confusione e della paura di non essere totalmente *compliant* rispetto al quadro regolatorio, evitando così in radice di correre il rischio di rispondere per eventuali danni.

La tecnologia dovrebbe velocizzare l'attività amministrativa e, il costante "dubbio giuridico", spesso alimentato dalla ipertrofia normativa, certamente non aiuta ad accelerare il procedimento.

In tale riflessione, occorre tenere presente che la amministrazione non si deve confrontare solo con il GDPR o il nuovo Regolamento IA: vi sono moltissimi testi normativi che in via diretta o indiretta trovano applicazione quando si tratta di digitalizzazione del pubblico in senso ampio: *i) in primis* il Codice sull'Amministrazione digitale, il quale norma anche le modalità di formazione o di firma del documento informatico; *ii)* le normative di settore che si applicano solo a particolari tipologie di dati oppure a determinati settori[23]; *iii)* la disciplina, anch'essa non priva di complicazione, delle norme di sicurezza informatica etc.

Sono, dunque, davvero molteplici i temi da tenere in considerazioni allorquando sia la pubblica amministrazione a trattare il dato personale.

2. Le peculiarità del trattamento dei dati da parte dei soggetti pubblici. Una ricognizione delle norme più rilevanti del GDPR in materia

Il GDPR è il testo normativo fondamentale per il trattamento dei dati personali e non perde la sua centralità nel sistema anche allorquando il trattamento sia effettuato da parte delle pubbliche amministrazioni nell'esercizio di funzioni pubbliche.

Il GDPR trova piena applicazione, difatti, anche nel settore pubblico e non solo relativamente alle

21. Cfr. Corte dei Conti, sezione giurisdizionale di Bolzano, 9 gennaio 2024, sentenza n. 1. La vicenda trae origine da una sanzione irrogata dal Garante per la protezione dei dati personali al comune di Bolzano con provvedimento n. 190 del 13 maggio 2021«per la violazione dell'art. 5, par. 1, lett. a) e c), 8, 9, 35, 13 e 88 del Regolamento europeo n. 2016/679, nonché degli artt. 113 e 114 del codice della privacy, avendo il comune posto in essere trattamenti di dati personali dei dipendenti relativi alla navigazione in internet, in assenza dei presupposti e di idonea informativa, e adottato una modulistica per la fruizione del servizio di assistenza psicologica non conforme al quadro normativo in quanto prevedeva la conoscenza di dati personali sullo stato di salute dei dipendenti da parte dei soggetti delegati allo svolgimento delle funzioni datoriali. In particolare, segnalava che i due presunti responsabili nella loro qualità, rispettivamente, di titolare del trattamento dei dati e di responsabile dei procedimenti amministrativi in materia di protezione dei dati personali e, dal 25 maggio 2018, Privacy Manager, non si sarebbero attivati per verificare la conformità della disciplina regolamentare interna a seguito dell'avvenuto mutamento del quadro normativo operato dal d.lgs. 4 settembre 2015, n. 151, neanche a seguito della pronuncia del Garante del 13 luglio 2016 (Trattamento dei dati dei dipendenti mediante posta elettronica e altri strumenti di lavoro), e non sarebbero intervenuti per eliminare le forme di trattamento dei dati personali illeciti neppure in sede di adozione delle "Linee guida per le procedure di adeguamento del GDPR 2016/679». Alla luce della vicenda così sintetizzata la Corte dei conti ha ritenuto sussistente la responsabilità erariale con riguardo alla funzionaria quale responsabile dei procedimenti amministrativi in materia di protezione dei dati personali, poi nominata Privacy Manager. La Corte ha ravvisato nei confronti di quest'ultima una colpa grave omissiva per non essersi attivata, nonostante la nomina che le imponeva di verificare la conformità normativa; di talché è stato ritenuto provato e sussistente l'elemento psicologico della "colpa grave".
22. Per un'analisi del fenomeno della burocrazia difensiva si vedano: Cantone-Carloni 2018.
23. Sul punto, ad esempio, una normativa speciale sulla digitalizzazione che si occupa anche di alcune tematiche di privacy è rappresentata dal Nuovo codice dei contratti pubblici. Cfr. Ferrari-Morbidelli 2023.

norme dedicate all'amministrazione ma anche con riferimento alle norme di carattere generale.

È stato, difatti, evidenziato che, oltre alle norme dedicate alle attività pubblicistiche, alle pubbliche amministrazioni «rimangono applicabili tutti quegli obblighi generali cui sono assoggettati i titolari di trattamento privati»[24]. Si giunge a tale considerazione in maniera abbastanza immediata ed agile sulla base dell'analisi delle norme dello stesso GDPR: a partire dalla stessa definizione di «titolare del trattamento» ove viene richiamata l'autorità pubblica senza ulteriori specificazioni «od esclusione in ragione del tipo di attività svolta»[25].

I principi generali[26], dunque, possono e devono essere applicati nell'ambito delle attività pubblicistiche; pertanto, ai sensi dell'art. 5 del GDPR[27], le amministrazioni devono rispettare:

(i) il *principio di liceità, correttezza e trasparenza*[28] in base al quale il trattamento di dati personali deve essere lecito, quindi, autorizzato dalla legge. La trasparenza viene intesa in tale contesto nel senso che le persone fisiche devono avere informazioni chiare ed esatte circa le modalità di trattamento;
(ii) il *principio di limitazione delle finalità* che impone che i dati siano raccolti «per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità» (cfr. art. 5, par. 1, lett. b) GDPR);
(iii) il *principio di esattezza* che impone alle pubbliche amministrazioni di adottare tutte le misure ragionevoli al fine di eliminare o rettificare in modo tempestivo i dati inesatti;
(iv) il *principio di minimizzazione dei dati* secondo cui è necessario limitare, il più possibile, il trattamento dei dati personali necessari al fine di raggiungere la finalità (cfr. art. 5, par. 1, lett. c) GDPR);
(v) il *principio di limitazione della conservazione*: il principio è strettamente connesso al principio di minimizzazione dei dati e implica che il tempo di conservazione sia il minimo necessario per conseguire la finalità;
(vi) *integrità e riservatezza*: le pubbliche amministrazioni devono garantire che i dati siano trattati in modo da garantire la necessaria sicurezza degli stessi, adottando le opportune misure tecniche e organizzative.

Ferma restando l'applicazione di tali principi generali sia per le attività privatistiche che pubblicistiche, come anticipato, non possono, tuttavia, essere taciute le peculiarità della normativa privacy applicabile al soggetto pubblico (o privato quando svolge attività di rilevanza pubblicistica)[29].

Una prima caratteristica generale da sottolineare è che il regime pubblicistico del trattamento dei dati, rispetto a quello privatistico, è maggiormente rimesso alla discrezionalità degli Stati membri e, dunque, le discipline nello spazio eurounitario risultano maggiormente diversificate.

Il GDPR, difatti, ha recepito l'esigenza di lasciare ampio margine di libertà agli Stati allorquando il trattamento dei dati sia connesso con la gestione di assetti pubblicistici. Ciò si deduce già dalla lettura dei considerando, in particolare, del considerando 10 nella parte in cui chiarisce che: «per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è

24. Cfr. D'Ancona 2018, p. 4 e Carullo 2020, pp. 131-163.
25. *Ivi*, p. 132.
26. In questa sede, si è scelto di soffermarsi sui principi generali in materia di privacy come selezionati nell'ambito dell'art. 5 GDPR.
27. Per una ricostruzione del contenuto dei principi evidenziati si veda Ponti 2023, p. 18.
28. Cfr. considerando 39.
29. Lo si ribadisce: la classificazione fatta propria dal GDPR per distinguere la disciplina applicabile ad un certo titolare del trattamento è sostanziale: *ex multis*, cfr. Granmar 2021, p. 230: «(a)s a starting point, any natural or legal person can shoulder the role as 'controller' since there are no inherent characteristics that distinguish the legal entity called controller from other natural or legal persons. It is the fact that the legal entity 'determines the purpose and means of the processing of personal data' that classifies a 'natural or legal person, public authority, agency or other body' among controllers. This causes the EDPB to advocate a casuistic and factual rather than formal conceptual construction».

investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento»[30].

Tale peculiarità, che stride con la volontà che ha guidato il legislatore eurounitario all'adozione del Regolamento, quella cioè di assicurare una disciplina il più possibile uniforme tra gli Stati, si spiega in considerazione di più fattori, alcuni più politici che giuridici[31].

Tuttavia, un fattore preliminare – prettamente giuridico – da considerare consiste nel fatto che le tradizioni di diritto amministrativo dei vari membri dell'Unione sono, di base, molto variegate, con una conseguente maggiore difficoltà di *reductio ad unum*.

Quindi, la prima peculiarità del trattamento dei dati personali nell'ambito pubblicistico è costituita proprio dall'assenza di una normativa europea davvero uniforme alla luce dei margini di discrezionalità lasciati, dallo stesso Regolamento, agli Stati[32].

Oltre alla menzionata peculiarità di carattere generale, la disciplina privacy, nel pubblico, assume ulteriori specificità di disciplina.

Tra queste si può citare, innanzitutto, l'aspetto della base di liceità[33]: difatti, nell'esercizio delle sue funzioni, la PA si avvale principalmente di due delle basi di liceità enucleate dall'art. 6: (*i)* l'obbligo legale e (*ii)* la necessità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di un titolare di trattamento[34] in forza dell'art. 6, par. 1, rispettivamente lett. c) ed e)[35].

Tali basi di liceità possono essere previste, oltre che dal diritto dell'Unione, anche dal diritto dello Stato membro (a riprova della rilevanza della normativa nazionale)[36].

Pertanto, mentre il privato si avvale, tradizionalmente, *in primis*, della base rappresentata dal consenso, le pubbliche amministrazioni o il privato che esercita funzioni pubbliche, solitamente, si avvalgono delle lettere c) ed e)[37].

Ciò non esclude, naturalmente, *tout court*, che la pubblica amministrazione possa trattare dati sulla scorta del consenso (o di altre basi giuridiche) ma esso presenta degli aspetti di criticità nel rapporto pubblicistico. Sul punto, è opportuno citare, oltre alla dottrina[38], il considerando 43 del GDPR laddove pone l'accento sulla minor probabilità che in un rapporto pubblicistico il privato presti un

30. Il tema dell'ampio "spazio di manovra" degli Stati è stato, a più riprese, sottolineato da attenta dottrina, *ex multis*, si veda Ponti 2023, p. 27.
31. Si rinvia, per una più compiuta ricostruzione, all'analisi di Ponti 2023.
32. Per una ricostruzione delle discipline in materia nei vari ordinamenti si veda, *ex multis*, Ponti 2023.
33. Cfr. Davies 2016, p. 294.
34. Cfr. Cardarelli 2021.
35. La lettera dispone che il trattamento è lecito quando «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento».
36. Il testo del GDPR è molto simile a quello della precedente Direttiva in materia, la n. 46 del 1995, all'art. 7, lett. e): «Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando (…) e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati». Tuttavia, nonostante le disposizioni siano pressoché identiche, molto diverso è l'impatto sui regimi nazionali delle fonti che contengono tali disposizioni (direttiva/regolamento).
37. Cfr. Carullo 2020, p. 131 «(n)é, del resto, parrebbe che tale previsione possa essere censurata alla luce del contesto normativo sovranazionale in cui si inserisce. Da un lato, la base giuridica del Regolamento è assicurata dall'art. 16 TFUE, dall'altro, l'art. 8, paragrafo 2, della Carta dei diritti fondamentali dell'Unione Europea ammette espressamente che i dati personali possano essere trattati, oltre che in base al consenso della persona interessata, anche sulla base di un altro fondamento legittimo previsto dalla legge».
38. Franca 2023, p. 341 «Si è avuto più volte modo di rilevare i limiti dovuti alla costruzione dei trattamenti sulla base di logiche consensuali, in ragione dello squilibrio informativo che contraddistingue il rapporto tra titolare e interessato».

consenso libero (cfr. considerando 43: «al fine di preservare la libertà di prestare il consenso, questo non può essere utilizzato come base giuridica qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica»)[39].

2.1. La base di liceità di cui all'art. 6, par. 1, lett. e)

Come anticipato, la lettera e) dell'art. 6, par. 1, è una delle basi di liceità più utilizzate dalle amministrazioni ed è anche una di quelle norme che ha destato maggiori tensioni con i principi di diritto amministrativo, in particolare, il principio di legalità.

È, dunque, opportuno effettuare un passo indietro per poi inquadrare tali *querelle*; il GDPR, per ritenere lecito il trattamento effettuato ai sensi della lett. e), richiede l'integrazione di specifici requisiti: innanzitutto, il trattamento in oggetto deve essere «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento». In secondo luogo, il GDPR impone il rispetto di un secondo requisito per avvalersi della lettera e) citata: l'esecuzione di tale compito pubblicistico può giustificare un trattamento se esiste una norma, nazionale o eurounitaria, di copertura (in forza dell'art. 6, par. 3, lett. b).

Il primo requisito fa riferimento alla c.d. clausola di necessarietà. Tale clausola non si applica solo in relazione alla lettera e) bensì a tutte le basi di liceità contenute nell'art. 6: essa implica che il trattamento sia lecito nella misura in cui si ponga come necessario per la realizzazione dell'attività in vista del quale viene effettuato (tale attività, come detto, può essere non solo l'esecuzione di un compito di interesse pubblico ma anche l'esecuzione di un contratto, l'adempimento dell'obbligo legale, la salvaguardia di interessi vitali e così via)[40].

Il secondo requisito, invece, chiarisce che la finalità pubblica nel trattare i dati non può essere presunta dalla mera qualifica, ad esempio, di soggetto pubblico[41] ma deve trovare un fondamento normativo[42], sia esso interno o eurounitario.

Orbene, tale secondo requisito è essenziale perché è tramite le norme – alle quali il Regolamento rinvia e che vanno a declinare il potere o lo scopo pubblico – che si riesce a comprendere quali finalità del trattamento sono perseguibili e, quindi, se è integrata o meno la base di liceità di cui alla lettera e).

Circa le caratteristiche che devono presentare le citate norme per poter fungere da adeguata base giuridica ai fini del trattamento si è sviluppato un dibattito in dottrina.

Infatti, tradizionalmente si afferma che, in forza del GDPR, è sufficiente che la base giuridica assegni all'amministrazione un certo potere pubblico o, addirittura, la tutela di un certo interesse o scopo pubblico. In altri termini, non è richiesto che la base giuridica disciplini anche il trattamento dei dati, individuando le finalità di trattamento ammissibili alla luce di un certo potere pubblico[43].

Ciò implica che se la PA ha il potere, ad esempio, di adottare un provvedimento di aggiudicazione di

39. Per una disamina del tema del consenso nell'ambito dei rapporti autoritativi privati/pubbliche amministrazioni: Carullo 2017, p. 48 ss.
40. Per approfondire si veda Ponti 2023 il quale si sofferma sul rapporto tra la clausola di necessarietà e il principio di legalità dell'azione amministrativa, ponendo altresì in luce come, in verità, il modo in cui opera la clausola di necessarietà riprende il meccanismo di funzionamento del potere implicito in quanto la norma si limita a fissare uno scopo e non il potere strumentale al raggiungimento dello scopo.
41. Sotto questo profilo, esiste una profonda differenza rispetto al regime precedente, soprattutto alla luce di come era stato declinato in Italia: la Direttiva 95/46/CE prevedeva che fossero leciti quei trattamenti necessari «per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» e, non faceva riferimento ad una norma specifica di copertura ma, era sufficiente, che quel trattamento rispondesse ad uno degli scopi pubblici perseguiti da un certo ente pubblico.
42. Il GDPR ha ripreso all'art. 6, par. 1, lett. e) il disposto della Direttiva 95/46/CE, all'art. 7 comma 1 lett. e). Tuttavia, nonostante la assimilabilità delle due disposizioni, le stesse hanno un impatto profondamente diverso.
43. Cfr. così Allena–Vernile 2022.

un bando, implicitamente ha il potere di trattare anche i dati personali a tale fine.

Tuttavia, attenta dottrina ha rilevato come una simile impostazione si ponga in violazione del principio di legalità[44].

Tale dottrina rileva sul punto che lo schema del Regolamento, se così interpretato, risponde al modello del potere implicito[45] («(t)ale potere (quello speso nel trattamento dei dati personali ai fini dell'esercizio di compiti di interesse pubblico) si declina però secondo lo schema del potere implicito, dal momento che esso non risulta attribuito esplicitamente dalla norma, ma assegnato in modo innominato: sono leciti tutti i trattamenti che risultino necessari all'esecuzione di un compito di interesse pubblico ovvero connessi all'esercizio di pubblici poteri»[46]).

Si tratta, dunque, di uno schema che, lo si ripete, non sembra totalmente conforme al principio di legalità, specie se si considera la legalità in senso forte, come declinata dalla più accreditata dottrina e giurisprudenza[47], in base al quale la legalità dell'azione pubblica – per dirsi rispettosa degli standard dello Stato di diritto – deve non solo attribuire il potere in modo esplicito ma anche descriverne le modalità di esercizio.

È pur vero che, per converso, richiedere per ogni trattamento che sia autorizzato e disciplinato da una specifica norma di legge rischia di essere molto gravoso per il sistema nel suo complesso.

A tal proposito, una parte della dottrina evidenzia come la tesi più rigida, c.d. dualista, a parte essere complessa sul piano applicativo, sarebbe *tout court* da escludersi su una base puramente teorica. Sul punto, viene sottolineato che tale interpretazione andrebbe, nella sostanza, a rendere inutile in radice la differenza tra le basi giuridiche dell'obbligo di legge e l'esecuzione del compito di rilievo pubblicistico, facendole nella sostanza coincidere e privando, in tal modo, di significato innovativo dell'ordinamento la base giuridica costituita dall'esecuzione del compito pubblicistico[48].

Vale la pena evidenziare che la richiamata impostazione sembra muovere, in radice, da una diversa categorizzazione del potere di trattamento dei dati da parte dei soggetti pubblici. Più nello specifico,

44. Per una puntuale ricostruzione della questione si veda Ponti 2023, p. 48 ss.

45. La teoria dei poteri impliciti deve molto alla tradizione giuridica statunitense: difatti, all'art. 1, sez.8, ult. comma della Costituzione Usa, viene riconosciuto al Congresso il potere di emanare ogni legge necessaria e opportuna al fine di esercitare i poteri tipici: «(t)o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof».

46. Ponti 2023, p. 47.

47. Per quanto concerne il principio di legalità nel diritto amministrativo, il tema ha una portata molto ampia e non può essere trattato in tale contesto e sul punto si rimanda alla enorme letteratura sul punto. Tuttavia, in sintesi, si rileva che, come noto, il principio di legalità può essere concepito in tre diverse accezioni: la prima è la c.d. legalità debolissima, la seconda quella debole e la terza c.d. forte. Per la prima accezione, l'amministrazione può fare tutto quello che non è vietato dalla legge. Per la seconda, il potere amministrativo deve avere un fondamento legale. In ultimo, l'accezione della legalità in senso forte, anche detta in senso sostanziale, implica che non sia sufficiente che vi sia una legge che riconosce il potere ma la stessa deve disciplinare il potere in questione, disciplinando le modalità di esercizio dello stesso. Tale accezione è stata confermata dalla Corte costituzionale in molteplici occasioni (cfr. *ex multis*, sentenze 307/2003, 32/2009, 115/2011). La ragione di tale posizione della Corte si spiega in quanto un principio di legalità solo formale andrebbe a lasciare troppa discrezionalità in capo alla PA così, *de facto*, non andando a tutelare i soggetti destinatari dell'azione amministrativa.

48. Franca 2023, p. 90 laddove evidenzia che: «(s)e, infatti, il trattamento per l'esecuzione di un compito a rilevanza pubblica richiede una norma espressa che lo legittimi, non si capirebbe in che modo una simile norma si differenzierebbe da quella che disciplina come obbligatorio un trattamento. È evidente invece che in un caso (quello dell'obbligo di legge) c'è una norma che disciplina un obbligo di trattamento, consumando qualsiasi valutazione in ordine all'*an* del trattamento, mentre nell'altro caso (compito a rilevanza pubblicistica) la norma rileva per disciplinare il compito a rilevanza pubblicistica in sé, mentre il trattamento è consentito se necessario a perseguire il compito a rilevanza pubblicistica previsto dalla norma».

tale lettura, sembra ritenere che il potere di trattare il dato personale non costituisca un autonomo potere pubblicistico ma una sorta di potere "neutro", strumentale a quello pubblicistico. Dunque, aderendo alla predetta tesi, si supera in radice la *querelle* della conformità del suddetto potere di trattamento con il principio di legalità o, in generale, con i tradizionali canoni pubblicistici[49].

Sulla base di tale premessa, sarebbe solo il potere pubblico "effettivo", che è quello che attribuisce la finalità pubblicistica al trattamento, che deve rispondere ai canoni imposti per l'attività amministrativa[50].

In ogni caso, a prescindere dalla menzionata questione, il GDPR chiarisce che le norme, su cui si fonda il trattamento, possono poi andare ad aggiungere ulteriori elementi da tenere in considerazione; per esempio, esse possono prevedere: condizioni di liceità del trattamento, categoria di dati suscettibili di trattamento, periodi di conservazione dei dati, misure di garanzie e di protezione del dato personale etc.

È proprio nella fase di dettaglio che si esplica il potere degli Stati, il loro spazio di manovra (in Italia, il legislatore ha deciso di esercitare il suo spazio di manovra, scelta opzionale e non necessitata, a differenza del precedente regime delineato dalla Direttiva 95/46/CE, da ultimo, con il d.lgs. n. 101 del 2018, come modificato nel 2021[51]).

Si noti che, alla stregua di quanto chiarito al considerando 41 del regolamento, la base giuridica non deve essere necessariamente una fonte primaria ma è sufficiente che tale base giuridica, anche di altro livello nella gerarchia delle fonti, sia chiara, precisa e accessibile e la sua applicazione possa essere prevedibile per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo. In questo senso, il legislatore italiano, nel 2021, nel riformulare l'art. 2-*ter*, co. 1 del Codice privacy, *sembrerebbe* aver previsto che la base giuridica rilevante per i trattamenti relativi all'esecuzione di compiti a rilevanza pubblicistica possa essere disciplinata non solo da una norma di legge o regolamento, ma da atti amministrativi generali[52].

Sempre in quel contesto riformatore del 2021, lo stesso è andato poi anche a specificare, affermando la bontà della prima tesi esposta che riprende il

49. Ad esempio, se l'amministrazione tratta i dati personali nell'ambito della procedura concorsuale, il trattamento dei dati *ex se*, non costituirebbe un vero e proprio potere autoritativo e, quindi, non sarebbe soggetto ai canoni del diritto amministrativo.

50. Franca 2023, p. 99: «(i)n particolare, il fatto che l'azione della pubblica amministrazione sia soggetta al principio di legalità spiega perché non sia necessario (e, anzi, si riveli pleonastico) richiedere che la norma di disciplina dell'attività amministrativa sia "doppiata" da una norma che disciplina i trattamenti ad essa connessa: in tal modo, infatti, si perverrebbe ad un aggravio eccessivo e ingiustificato. Se la norma disciplina un potere o un compito dell'amministrazione rispetto a cui il trattamento di dati si pone in chiave di strumentalità necessaria, è giocoforza che la norma stessa costituisca la base del trattamento».

51. Per una ricognizione dell'esperienza italiana, la quale ha oscillato da un estremo all'altro nelle scelte regolatorie del settore si rimanda a Ponti 2023, p. 92 ss. L'autore, sul punto, a p. 95 del citato scritto evidenzia che: «(m)entre in precedenza si statuiva che il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari fosse consentito anche in mancanza di una norma di legge o di regolamento che lo prevedesse espressamente, la nuova formulazione utilizza l'avverbio esclusivamente, ciò che è stato inteso nel senso di attrarre nella base giuridica non solo la qualificazione della fonte ("esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento"), ma anche ciò che in precedenza poteva restare fuori dalla fonte legislativa ("Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito (…) anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente"). In base a questa lettura, pertanto, la base giuridica (legislativa, o regolamentare, se a ciò espressamente abilitata) non può limitarsi ad individuare ed affidare al titolare del trattamento l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri, ma deve (quantomeno) prevedere espressamente quale trattamento (di quali dati, e per quale finalità) possa essere realizzato».

52. Per una sintesi dei tratti distintivi tra regolamento e atto amministrativo generale si veda Consiglio di Giustizia amministrativa per la Regione siciliana, 14 marzo 2011, n. 200, che a sua volta richiama l'Adunanza Plenaria del Consiglio di Stato.

meccanismo di funzionamento dei poteri impliciti, che il trattamento «è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti» (cfr. art. 2-*ter* co. 1-*bis*)[53].

Recente dottrina ha, tuttavia, evidenziato che la riforma italiana non sarebbe pienamente conforme al GDPR in quanto lo stesso «pur lasciando agli Stati membri la scelta su quali misure adottare per specificare l'applicazione del Regolamento 2016/679/UE, richiede tassativamente che la base giuridica del trattamento dei dati personali sia proporzionata all'obiettivo legittimo perseguito»[54]. In altri termini, secondo la citata impostazione, la normativa italiana non sarebbe compatibile con la fonte eurounitaria in quanto, *de facto*, con l'ultimo intervento normativo del 2021, il legislatore italiano ha autorizzato, in via generale, il trattamento di dati personali e lo scambio di tali dati tra autorità pubbliche ogniqualvolta questo sia necessario per il perseguimento di fini istituzionali, senza menzionare il principio proporzionalità tra trattamento dei dati e fini pubblici perseguiti, espressamente richiesto dal GDPR.

Peraltro, la riflessione dottrinaria riportata può costituire spunto per effettuare un'ulteriore valutazione relativa al rispetto del canone di proporzionalità interno sotteso all'azione amministrativa[55].

L'amministrazione è, inoltre, tenuta: (i) a fornire corretta informativa circa le finalità del trattamento, i tipi di dati raccolti, i destinatari e i loro diritti di protezione dei dati; (ii) alla nomina di un responsabile della protezione dei dati; (iii) a predisporre le opportune misure di sicurezza per proteggere i dati dall'esterno (attacchi *hacker* etc.).

Ancora, norma fondamentale per il corretto rispetto dall'assetto delineato dal GDPR da parte delle pubbliche amministrazioni è l'art. 30. In base a tale disposizione, le pubbliche amministrazioni devono adottare il registro dei trattamenti che deve contenere: il nome e i dati di contatto del titolare del trattamento e del DPO; le finalità del trattamento; la descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; i termini ultimi previsti per la cancellazione delle diverse categorie di dati; una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione.

Già in base a tale breve ricognizione del sistema del GDPR si possono dedurre due aspetti: il primo è che il regime pubblicistico del trattamento dei dati, ferma l'applicazione dei principi generali, presenta delle peculiarità molto rilevanti; il secondo è che tale regime, anche solo osservando la disciplina del GDPR, non è del tutto lineare e, spesso, non combacia con i principi generali (per esempio, principio di legalità) dell'azione amministrativa.

3. Il Regolamento sulle intelligenze artificiali: la filosofia di fondo

Come è noto, l'Unione europea ha adottato[56] la prima regolamentazione in materia di intelligenza artificiale[57].

L'adozione del Regolamento si colloca nell'ambito di una più ampia strategia europea volta a governare il mercato dei dati[58]. In questo senso, il

53. Francario 2021.

54. Carullo 2024.

55. Tuttavia, la preoccupazione evidenziata dalla dottrina richiamata cfr. Carullo 2024 sembra essere superata considerando che l'art. 2-*ter* del Codice privacy, come risultante dall'ultima modifica intercorsa, richiama espressamente l'art. 6 GDPR, il quale richiama, a sua volta, il principio di proporzionalità.

56. Si tratta del Regolamento n. 1689/2024.

57. Nonostante sia recente il massivo riferimento al concetto di *Artificial Intelligence* (AI) sia a livello mediatico che accademico, tale concetto non è così nuovo. Il termine è stato coniato negli anni Cinquanta del secolo scorso, in un contesto accademico, per indicare un campo di ricerca emergente che studia: (i) la capacità delle macchine di svolgere compiti mostrando un comportamento intelligente simile a quello umano; e (ii) la capacità delle macchine di comportarsi come agenti intelligenti percependo l'ambiente e prendendo decisioni per raggiungere determinati obiettivi cfr. Medaglia–Gil-Garcia–Pardo 2023.

58. La strategia europea per i dati ha preso le mosse da una comunicazione della Commissione europea del 19 febbraio 2020, COM(2020) 66, ove si evidenziava la centralità dei dati in quanto gli stessi rappresentano «(…) la

Regolamento è solo una delle iniziative che dovrebbe concorre a creare una gestione unica del mercato dei dati nello spazio dell'Unione europea[59]. Uno dei comuni denominatori delle iniziative citate è il riconosciuto valore patrimoniale del dato quale linfa vitale per il funzionamento delle nuove tecnologie: il legislatore eurounitario, difatti, sebbene tuteli il diritto alla privacy e, quindi, i dati personali[60], è consapevole delle istanze delle imprese europee e dell'esigenza di renderle competitive a livello mondiale. Il riconosciuto valore patrimoniale del dato emerge già in sede di considerando (in particolare dai considerando 3 e 4) laddove si evidenzia la centralità strategica nell'implementazione della tecnologia e, in particolare, della famiglia delle intelligenze artificiali «contribuendo al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi»[61].

Chiarito che il Regolamento sulle IA non è un'iniziativa *stand alone*, bisogna pur evidenziare che la stessa assume un particolare significato anche considerata singolarmente, un significato prima politico che giuridico[62] poiché, come evidenziato da gran parte della dottrina intervenuta anche ante adozione del testo definitivo[63], soprattutto alla luce del fatto che si tratta del prima fonte di carattere

linfa vitale dello sviluppo economico: sono la base di molti nuovi prodotti e servizi e generano guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici, rendendo possibili prodotti e servizi più personalizzati, un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici. Sono, inoltre, una risorsa essenziale per le start-up e le piccole e medie imprese (PMI) per quanto concerne lo sviluppo di prodotti e servizi. La disponibilità di dati è essenziale per l'allenamento dei sistemi di intelligenza artificiale, con prodotti e servizi in rapida evoluzione, da riconoscimento morfologico e insight generation a tecniche di previsione più sofisticate e, di conseguenza, decisioni migliori».

59. Tra gli atti normativi che confluiscono nella regolazione del settore si possono citare: il *Data Governance Act*; il *Data Act*; il *Digital Services Act* e il *Digital Markets Act*. Si rimanda, per un'analisi più approfondita a Falletta–Marsano 2024, p. 121.

60. *In primis* tramite il GDPR ma anche, come noto, negli anni, un importantissimo strumento di protezione è stata (ed è) la Convenzione europea dei diritti dell'uomo, in particolare in forza dell'art. 8, insieme alle relative pronunce della CEDU.

61. Cfr. considerando 4 Regolamento IA.

62. L'Europa, come evidenziato in premessa, si è attribuita il ruolo di leader mondiale di regolazione del fenomeno. La definizione di sistema di intelligenza artificiale di cui all'articolo 3, paragrafo 1 è stata modificata per allinearla maggiormente al lavoro delle organizzazioni internazionali che si occupano di intelligenza artificiale, in primis l'OCSE. Di ciò si ritrova traccia nel considerando 12 del Regolamento: «la nozione di «sistema di IA» di cui al presente regolamento dovrebbe essere definita in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale (…)».

63. De Gregorio–Paolucci–Pollicino 2021.

generale e di *hard law* al mondo[64], l'Unione europea si è posta come leader nella regolazione del settore a livello mondiale. A riprova del ruolo di *leadership che ha assunto il diritto unionale*, occorre evidenziare, senza pretese di completezza, come l'esperienza di altre legislazioni mondiali, sebbene intervenute in materia, abbiano un impatto minore. Per esempio, negli Stati Uniti, nell'ottobre 2023, l'amministrazione Biden ha emesso un *Executive Order* avente ad oggetto l'uso sicuro e protetto dell'intelligenza artificiale: *Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*[65].

Orbene, tale intervento, non ha la medesima forza dell'*AI Act* e ciò sotto almeno due punti di vista.

In primo luogo, non è equivalente dal punto di vista della qualità della fonte: difatti, l'*executive order* non ha la forza e la stabilità di un Regolamento eurounitario. L'*executive order* è un atto dotato di coattività ma è imputabile al solo esecutivo, in particolare al Presidente degli Stati Uniti, senza che vi sia alcuna "ratifica" da parte del Parlamento. Ciò significa che è, per sua natura, meno stabile. Inoltre, tale fonte può rivolgersi solo agli organi dell'esecutivo stesso e, quindi, non può regolare direttamente gli organi posti al di fuori dell'esecutivo o i soggetti privati[66].

Sotto il profilo, invece, contenutistico mentre l'*AI Act* pone numerosi e specifici obblighi, l'*Executive Order* non contiene particolari oneri o prescrizioni ma, tendenzialmente, si "limita" ad esporre dei principi generali e a prevedere lo sviluppo di linee guida e di *best practices* da parte delle amministrazioni. Si può, quindi, affermare che l'approccio statunitense al tema sia più *soft*[67].

L'impatto del Regolamento IA, tuttavia, non si esaurisce nel significato politico e di *leadership* europeo: infatti, lo stesso sottende una precisa scelta regolatoria che possa bilanciare le esigenze di avanzamento tecnologico con il rispetto dell'uomo. Rispetto dell'uomo che non pare intendersi solo come rispetto dei diritti umani ma anche come tutela della "centralità umana" in ogni processo che abbia un impatto rilevante.

In questo senso, almeno "a parole", il regolamento sembra richiamare dei concetti di diritto naturale volendo «rimodulare il perimetro del tecnicamente possibile sulla base di quello che si ritiene giuridicamente ed eticamente accettabile»[68].

La nuova disciplina, dunque, ha recepito un'impostazione antropocentrica dell'intelligenza artificiale[69]: l'uomo dovrebbe essere al centro della rivoluzione tecnologica. Ciò viene confermato anche dall'art. 14 del Regolamento, dedicato alla

64. Prima dell'adozione del regolamento vi erano stati molteplici tentativi, anche europei, di regolare tramite *soft law*: tra questi, le *Linee guida relativa ai principi sull'intelligenza artificiale* dell'OCDE e la raccomandazione del Consiglio d'Europa adottata il 14 maggio 2019 (si tratta di una regolamentazione che «aveva mantenuto il livello della discussione sul piano dei principi»). Nel 2021, si è compiuto poi il passaggio cruciale mediante la Risoluzione del Parlamento europeo sull'intelligenza artificiale e con la presentazione del Regolamento IA poi approvato, in via definitiva, dal Parlamento europeo, il 13 marzo del 2024.

65. Oderlberg 2024.

66. Cfr. Esposito 2023 e Pollicino 2023.

67. Colpisce, inoltre, la considerazione del peso dei privati nello sviluppo regolatorio sul tema. Si legge, nel testo del provvedimento del Presidente Biden, che «executive departments and agencies shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations».

68. Anche se il valore etico ed antropocentrico è stato oggetto di riflessioni della dottrina ante adozione, cfr. De Gregorio–Paolucci–Pollicino 2021.

69. Il primo considerando del Regolamento indica, in questo senso, che il suo scopo è quello di «migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»),

"Sorveglianza umana", nell'ambito del quale si evidenzia la necessità, per i sistemi di alto rischio, di un pregnante controllo da parte dell'uomo.

3.1. Le norme del Regolamento IA più rilevanti per l'attività pubblicistica

Il Regolamento, già nei suoi considerando, si dimostra sensibile al tema del rapporto tra gli interessi pubblici ed i connessi rischi applicativi delle intelligenze artificiali.

Il considerando 5, difatti, evidenzia come l'intelligenza artificiale possa «(…) a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico»[70].

In questo senso, il considerando 7 rileva che è fondamentale costituire un quadro giuridico armonizzato in tale materia al fine di garantire che lo sviluppo delle IA non vada a sacrificare «un elevato livello di protezione degli interessi pubblici».

Ancora, il considerando 167 afferma che i soggetti chiamati ad applicare il regolamento devono fare in modo di operare nel rispetto della riservatezza al fine di garantire «l'integrità del procedimento amministrativo».

Alla luce di ciò, è possibile evidenziare la piena consapevolezza, da parte del legislatore eurounitario, della specialità del settore pubblico, soprattutto in considerazione dei maggiori rischi sull'impatto dei diritti, che l'utilizzo di una tecnologia avanzata nel settore pubblico potrebbe comportare.

Ciononostante, l'impalcatura del Regolamento non prevede dei regimi apertamente differenziati tra l'uso delle tecnologie nell'attività privata o nell'attività pubblicistica ma li regola insieme, sebbene vi siano delle norme, come si vedrà, che hanno principalmente una vocazione pubblicistica.

È opportuno, dunque, in estrema sintesi, muovere dall'analisi delle principali norme del Regolamento.

L'art. 3 del Regolamento reca la definizione di sistema di IA da intendersi come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[71].

Alla luce di ciò, un sistema di IA rientra nell'ambito di applicazione del Regolamento allorquando (i) presenti un qualche livello di autonomia rispetto all'uomo, (ii) abbia una qualche capacità di apprendimento, potendo generare sulla base degli input, degli output, (iii) gli output devono poter influenzare un ambiente fisico o virtuale.

La normativa neo approvata si fonda su un *risk based approach*: ossia, vengono distinte le intelligenze artificiali a seconda del pericolo che le stesse potrebbero causare ai diritti fondamentali[72].

Più alto è il rischio più la regolamentazione è stringente.

Il considerando 48 chiarisce che, per valutare l'impatto in termini di rischio, uno strumento importante è rappresentato dalla Carta dei diritti fondamentali dell'Unione europea: «(l)a portata dell'impatto negativo del sistema di IA sui diritti

compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione (…)» (cfr. anche art. 1 del Regolamento).

70. Cfr. considerando 5.

71. Sulla definizione di IA cfr. Martinez 2019 e Wang 2019.

72. Puckzo 2024: «The European Union (EU) has been at the forefront of regulating AI ethics, primarily through the General Data Protection Regulation (GDPR) and the proposed AI Act. The GDPR, enacted in 2018, sets stringent guidelines on data protection and privacy, directly impacting AI systems that process personal data. Key principles of the GDPR include data minimization, purpose limitation, and the right to be informed about automated decision-making. These principles ensure that AI systems are designed with privacy in mind, protecting individuals' data from misuse and unauthorized access. In addition to the GDPR, the EU has proposed the AI Act, which seeks to establish a comprehensive legal framework for AI. The AI Act categorizes AI applications into different risk levels (unacceptable, high, and minimal risk) and imposes corresponding regulatory requirements».

fondamentali protetti dalla Carta è di particolare rilevanza ai fini della classificazione di un sistema di IA tra quelli ad alto rischio. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione».

Andando più nello specifico, all'interno del Regolamento, si distinguono quattro principali tipologie di rischio:

(i) *Il rischio è inaccettabile* e, dunque, l'uso delle IA è totalmente vietato. A tal fine, è l'art. 5 che elenca le pratiche IA vietate. In base alla citata norma sono vietati, *ex multis*: i sistemi di IA che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli volte a distorcere il comportamento delle persone (cfr. art. 5, par. 1, lett. a); i meccanismi di sfruttamento delle persone vulnerabili (cfr. art. 5, par. 1, lett. b); i sistemi di IA che introducano meccanismi di *scoring* sociale (cfr. art. 5, par. 1, lett. c)[73]; i sistemi che effettuino indagini di polizia predittiva, con alcune eccezioni (cfr. art. 5, par. 1, lett. d)[74]; categorizzazione biometriche da cui dedurre razza, convinzioni religiose politiche o filosofiche, orientamenti sessuali etc. (cfr. art. 5, par. 1, lett. g); i sistemi che possano interferire relativamente alla privacy mentale delle persone, sui luoghi di lavoro o di istruzione, decodificando emozioni e così via, con alcune eccezioni costituiti da motivi di salute o di sicurezza (cfr. art. 5, par. 1, lett. f); i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a meno che la ricerca non sia volta a fini specifici collegati alla sicurezza pubblica; tra i fini specifici, per esempio, si annoverano la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; la prevenzione di una minaccia specifica, come un attacco terroristico; ricerca di soggetti sospettati di aver commesso un reato grave etc. (cfr. art. 5, par. 1, lett. h).

(ii) *Il rischio è alto* e, dunque, si pongono a carico di produttori e sviluppatori di tali sistemi stringenti obblighi *ad hoc* che riguardano ogni fase del ciclo di vita della IA (progettazione, collaudo, monitoraggio, nonché responsabilità aggiuntive)[75]. il Regolamento impone poi, per i sistemi ad alto rischio, l'adozione di un sistema di gestione del rischio nonché l'obbligo di effettuare dei test e di garantire, oltre

73. Più precisamente, l'art. 5, par. 1, lett. c) si riferisce alla «(…) immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità».

74. La norma così dispone: «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»; la lettera f) che vieta «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza».

75. Cfr. artt. 9 e ss. del Regolamento.

alla citata sorveglianza umana, anche l'accuratezza, robustezza e cybersecurity. Il rispetto di tutti i menzionati requisiti è richiesto per il rilascio, da parte dell'Autorità competente, della valutazione di conformità dell'IA.

(iii) *Il rischio è basso* o minimo; simili tecnologie non sono sottoposte a particolari obblighi ma devono, comunque, garantire i principi della trasparenza e robustezza.

(iv) Sussiste un rischio specifico attinente alla tutela della trasparenza.

In base alla riassunta classificazione, si può effettuare, anche se "a caldo", con tutte le approssimazioni del caso, il seguente ragionamento.

Innanzitutto, è possibile notare che alcune tecnologie inaccettabili (IA a rischio inaccettabile) diventano accettabili allorquando siano volte a realizzare dei fini pubblicistici. Per esempio, come detto, il Regolamento vieta, all'art. 5, par. 1, lett. f), «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione» a meno che l'uso del sistema di IA sia volto a realizzare interessi pubblici della tutela della salute e della sicurezza (testualmente si legge nel Regolamento «motivi medici o di sicurezza»).

Quindi, talvolta, l'interesse pubblico potrebbe rendere più permissiva la disciplina applicabile.

Tuttavia, per converso, come ben esplicitato dal soprariportato considerando 48, per parametrare il rischio accettabile e il rischio non accettabile bisogna valutare anche l'impatto sui diritti fondamentali e, in particolare, anche il diritto ad una buona amministrazione. In questo senso, l'inserimento dell'uso dell'intelligenza artificiale nel procedimento amministrativo può rappresentare qualche complessità in più.

Quindi, in forza dei sintetici ragionamenti svolti, lo si ripete, con buona approssimazione, sebbene sia senz'altro vero che l'attività pubblicistica non presenti una disciplina generale differente o rafforzata rispetto a quella privata (come detto, il Regolamento non prevede che l'uso delle IA nell'ambito del potere pubblico comporti *ex se* un rischio più elevato) è pur vero che, sul piano della realtà, una intelligenza artificiale utilizzata per esercitare il potere pubblico presenterà, il più delle volte, un rischio maggiore per i diritti enucleati nella Carta dei diritti fondamentali dell'Unione europea.

Le peculiarità dell'attività pubblicistica nell'economia del Regolamento IA vengono in rilievo anche ai sensi dell'art. 27 dello stesso, relativa ai sistemi ad alto rischio. L'articolo 27 prevede che: «(p)rima di utilizzare un sistema di IA ad alto rischio (…) i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici (…) effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre». La norma chiarisce, inoltre, che tale valutazione debba comprendere una serie di elementi: a) una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

In base alla citata norma i *deployer* che esercitano attività pubblica e che utilizzano sistemi di IA ad alto rischio devono effettuare una valutazione di impatto sui diritti fondamentali (c.d. *Fundamental Rights Impact Assessment*, in breve FRIA)[76].

4. Il Regolamento IA e GDPR a confronto: analogie e differenze tra le due fonti

Porre a confronto il Regolamento IA e il GDPR è una operazione necessaria perché, come detto, l'utilizzo di IA presuppone, nella quasi totalità dei casi, trattare dati personali.

Per esigenze di chiarezza espositiva, nel prosieguo, si analizzeranno quelli che appaiono, a caldo, i principali punti di contatto nonché di divergenza.

76. La "vicinanza" tra la FRIA e l'obbligo descritto dal GDPR ai fini della redazione del *Data Protection Impact Assessment* sarà oggetto di trattazione nel paragrafo 4.1.

Relativamente alle similitudini, oltre alla forma normativa prescelta, il regolamento, i due testi condividono diverse caratteristiche.

Su un piano più politico che giuridico, in entrambe le esperienze regolatorie, l'Unione europea, adottando tali legislazioni molto innovative, ha dato prova del suo ruolo di *leadership* nella regolazione del fenomeno tecnologico a livello mondiale. In questo senso, si può ragionevolmente immaginare che il Regolamento IA, così come è stato per il GDPR[77], assumerà la funzione non solo di normare lo spazio europeo ma di assurgere a modello legislativo per le legislazioni mondiali[78].

Anche da un punto di vista contenutistico, si possono scorgere analogie tra i due strumenti. Tra queste similitudini, *in primis*, si può evidenziare la *centralità dei diritti fondamentali*: entrambi i regolamenti, nell'abito del rispettivo primo considerando, fanno espresso riferimento alla necessità di garanzia di tali diritti, menzionando la Carta dei diritti fondamentali dell'Unione europea.

Ciò era pure stato evidenziato dalla dottrina intervenuta prima dell'adozione del testo definitivo dell'*AI Act* la quale, avvalendosi di una «tassonomia usuale nell'ambito degli studi di comparative law and regulation»[79], ha evidenziato che il Regolamento sulle intelligenze artificiali è costruito su «un modello regolatorio non incentrato sulla logica della ballot-box democracy, né su quella della rule by law, bensì rispondente al paradigma dei diritti fondamentali»[80].

Nel dettaglio: (i) considerando 1 GDPR: «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»; (ii) considerando 1 Regolamento IA: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione».

Inoltre, in entrambi i regolamenti, la trasparenza assume una valenza significativa in quanto strumento essenziale al fine di tutelare i diritti fondamentali delle persone: il GDPR impone diversi obblighi di trasparenza sui processi di raccolta e trattamento dei dati e l'*AI Act*, allo stesso tempo, richiede che i sistemi di intelligenza artificiale, soprattutto se ad alto rischio, garantiscano la trasparenza e la spiegabilità del risultato. Quindi, "sul piano valoriale" i due Regolamenti muovono da presupposti molto simili. Da notare che in

77. Tra i tanti esempi di legislazione straniera che si sono ispirati al modello GDPR, si può citare la legge vigente in California, USA, il c.d. *Consumer Privacy Act* (CCPA) che è la più garantista legge sulla privacy negli Stati Uniti a livello dei singoli Stati (si noti che negli USA non esiste una legge federale generale in materiale). Per approfondire si veda: Barett 2019, p. 24.

78. Si è visto come un modello alternativo regolatorio, più *soft*, possa essere quello statunitense.

79. Bignami 2018.

80. Resta 2022, p. 323 il quale evidenzia la profonda rilevanza della tutela dei diritti fondamentali nell'economia della regolazione IA europea: «(i)l cardine della proposta sembra infatti risiedere nella definizione di un modello regolatorio finalizzato alla gestione ottimale dei rischi insiti nell'utilizzo dei dispositivi IA con l'obiettivo primario di tutela dei diritti fondamentali e di salvaguardia del processo democratico. Formule di spiccato valore retorico come quella della "human-centric" o "trustworthy-AI" riflettono plasticamente l'idea che le applicazioni di IA possono incidere sul sistema di protezione della dignità umana e dei diritti fondamentali, sicché un puro modello di self-regulation risulta inappropriato. È soltanto attraverso un approccio di hard law che può realizzarsi un accettabile bilanciamento tra la tutela della persona e altri interessi concorrenti, come quello della sperimentazione innovativa e della crescita economica».

entrambi i Regolamenti, nonostante la menzionata centralità della tutela dei diritti, si registra una sensibilità al tema del necessario bilanciamento tra tale tutela e altri interessi legati allo sviluppo economico: nel caso del GDPR, l'interesse con il quale controbilanciare la tutela dei diritti è la libera circolazione dei dati, nel caso dell'*AI Act*, è la garanzia di non arrestare lo sviluppo tecnologico. Ancora, GDPR e *AI Act* condividono una spiccata tendenza alla extraterritorialità. Sul punto, è sufficiente porre a confronto l'art. 3 del GDPR e l'art. 2 del Regolamento IA: essi si applicano non solo ai soggetti che sono stabiliti nell'Unione ma anche a soggetti che siano "collegati" al mercato europeo.

Inoltre, i due strumenti aderiscono al modello del *risk based approach*[81]: più è alto il rischio di violazione dei diritti fondamentali, più gravosi sono gli obblighi imposti agli utilizzatori. Si tratta, dunque, di schemi regolatori a «geometria variabile, dove i doveri di condotta e gli itinerari di enforcement vengono modulati in funzione dei diversi livelli di rischio prevedibilmente connessi a una determinata tipologia di attività»[82]. In questo senso, il Regolamento IA riprende ed enfatizza tale metodo di regolazione basato sul rischio che è proprio anche del GDPR, come emerge dall'analisi degli artt. 25 e 35 di quest'ultimo, ove si prevedono degli obblighi per i provider di mappatura del rischio e di adottare sistemi idonei a neutralizzarlo.

Tuttavia, iniziando ad addentrarci nell'analisi degli *elementi di dissonanza* tra i due regolamenti, la declinazione del modello del *risk based approach* è differente: nel GDPR la valutazione del rischio è decentralizzata, effettuata dai soggetti direttamente coinvolti e fondata sul principio di accountability, nell'ambito dell'*AI Act* è il legislatore eurounitario che tenta di creare una categorizzazione astratta dei livelli di rischio.

In aggiunta, a monte, si può riflettere, in termini generali, sulla difficoltà che l'applicazione congiunta dei due Regolamenti comporterà: i sistemi IA necessitano di enormi quantità di dati per funzionare e, in gran parte, si tratta di dati personali; per converso, il GDPR si fonda sul principio della limitazione delle finalità del trattamento[83], che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime e il relativo riuso non sia possibile se non negli stringenti limiti individuati dalla normativa. Garantire che i dati personali immessi (moli molto significative di dati) siano trattati in modo conforme alla finalità per i quali originariamente sono stati acquisiti è estremamente complesso, se non, materialmente, impossibile. La tensione tra il principio di finalità e i sistemi di intelligenza artificiale si è registrata anche nella fase di addestramento delle stesse. Per esempio, nel noto caso *Clearview AI*[84], il Garante per la protezione dei dati personali ha sanzionato la suddetta società per aver raccolto dati al fine di addestrare un algoritmo, in aperta violazione del principio di finalità.

Sempre muovendo dal rilievo in base al quale le intelligenze artificiali sono alimentate da big data, diventa complesso garantire un altro caposaldo del GDPR la minimizzazione dei dati: difatti, anonimizzare il dato personale oltre che costituire un'operazione complessa può incidere sulla precisione dell'analisi compiuta dalla macchina.

Alla luce di quanto rilevato, pertanto, soprattutto per le IA più evolute, come quelle che si basano sul machine learning «si è determinata una inevitabile tensione con i principi cardine della normativa sul trattamento dei dati, e segnatamente con i

81. Floridi 2021.

82. Resta 2022, p. 339.

83. In dottrina cfr. Mühlhof–Ruschemeier 2024 e Trozzi 2024 i quali hanno analizzato le tensioni tra il meccanismo di funzionamento delle intelligenze artificiali e il principio di limitazione delle finalità. Sul tema, può essere anche utile richiamare la giurisprudenza relativa alle incompatibilità tra il GDPR ed i c.d. usi secondari, facendo riferimento, in particolare, al caso Digi (CGUE, sentenza del 20 ottobre 2022, *Digi Távközlési és Szolgáltató Kft. contro Nemzeti*, C-77/21).

84. Cfr. Garante per la protezione dei dati personali, Registro dei provvedimenti n. 50 del 10 febbraio 2022. Un altro esempio, sul punto, è recente caso di ChatGPT, gestita da Open AI, nell'ambito del quale il Garante ha richiesto, dopo un'approfondita istruttoria, una serie di adeguamenti, anche per garantire il rispetto del principio di finalità (cfr. Garante per la protezione dei dati personali, Registro dei provvedimenti n. 755 del 2 novembre 2024).

principi di finalità e minimizzazione»[85]; pertanto, alla luce di ciò, le scelte regolatorie in tale settore sono sottoposte ad un compromesso necessario tra le esigenze di sviluppo tecnologico e l'esigenza di tutela degli individui. Talvolta, nel bilanciamento, prevale la tutela della privacy, altre volte, prevale l'esigenza nell'avanzare tecnologico, con tutti i benefici che ne conseguono (tra cui, la tutela di altri diritti, diversi dalla privacy).

Un esempio di prevalenza dello sviluppo tecnologico rispetto alla tutela del dato personale, si ritrova all'art. 10, par. 5, del Regolamento IA, con riferimento alla normativa sui dati particolari. Infatti, l'art. 10, introduce una eccezione al divieto di raccolta e trattamento dei dati particolari di cui all'art. 9 GDPR, quando ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche[86].

In chiusura, è necessario valutare una delle più evidenti sovrapposizioni tra GDPR e Regolamento IA, valutando il rapporto tra l'art. 22 GDPR e l'*AI Act*: difatti, l'art. 22 GDPR contiene una disciplina relativa ad una delle ipotesi di forme di trattamento dei dati personali tramite intelligenze artificiali, occupandosi del trattamento nell'ambito di processi decisionali automatizzati[87].

L'art. 22, par. 1, del GDPR vieta i trattamenti dei dati personali nell'ambito di processi decisionali automatizzati, compresa la profilazione, che producano effetti giuridici o che incidano significativamente sulla persona[88]. Tuttavia, non si tratta di un divieto generale, in quanto, al secondo paragrafo, ammette tali processi decisionali automatizzati in tre diverse ipotesi: quando il trattamento sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; quando il trattamento sia autorizzato dal diritto interno o eurounitario, purché si garantiscano adeguate misure a tutela dei diritti dell'interessato; oppure nell'ipotesi in cui il trattamento si basi sul consenso esplicito dell'interessato.

Al contrario, il Regolamento IA non contiene alcun divieto generale relativamente alle forme di intelligenza artificiale che implichino processi decisionali automatizzati ma, al contempo, alcuni dei processi decisionali automatizzati sono *tout court* vietati in quanto considerati a rischio inaccettabile (si pensi al caso dello *scoring* sociale).

Come evidenziato in dottrina[89], sicché alcuni processi decisionali automatizzati sono, in teoria, ammissibili per il GDPR e vietati *tout court* per il Regolamento IA, contrariamente a quanto si potrebbe credere, la disciplina del GDPR non è

85. Resta 2022, p. 335.

86. Il Regolamento richiede, tuttavia, che siano soddisfatte una serie di condizioni, che devono sussistere in modo congiunto, tra le quali, per esempio, il fatto che le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi.

87. In dottrina, *ex multis*, si veda Bolognini–Pelino 2024.

88. Moltissime sono state le pronunce della giurisprudenza amministrativa in tema di processi decisionali automatizzati nell'ambito delle quali si è ammesso l'uso di tali tecnologie, con espresso richiamo anche all'art. 22 GDPR, a condizione che si garantiscano i principi del procedimento, in primis la trasparenza, in virtù della particolare efficienza che le stesse comportano, in attuazione dell'art. 97 Cost. A titolo meramente esemplificativo, la giurisprudenza si è occupata di assegnazione o trasferimenti, mediante tali tecnologie, degli insegnanti, ammettendone l'uso. Si veda, *ex multis*, la pronuncia del Consiglio di Stato, sentenza n. 8472 del 2019, ove il massimo consesso della giustizia amministrativa ha evidenziato che: «(a)nche il caso in esame, relativo ad una procedura di assegnazione di sedi in base a criteri oggettivi, l'utilizzo di una procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata: essa comporta infatti numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata». In senso conforme, può richiamarsi la pronuncia del Consiglio di Stato n. 2270 del 2019.

89. Sul tema si veda Falletta–Marsano 2024, p. 128.

sempre più limitativa o stringente rispetto a quanto disposto nell'*AI Act*.

In ultimo, in sintesi, è opportuna una breve comparazione dell'impianto sanzionatorio dei due Regolamenti[90]. Invero, il Regolamento IA e il GDPR, sotto questo profilo, condividono una impostazione molto simile sia per i meccanismi di quantificazione della sanzione amministrativa, che per la discrezionalità riconosciuta alle Autorità di vigilanza chiamate ad applicare le sanzioni.

Sotto il primo profilo, in entrambi i casi la determinazione della sanzione è effettuata mediante una percentuale del fatturato[91] del soggetto destinatario della sanzione. La percentuale è determinata in ragione della gravità della violazione. Inoltre, entrambi i sistemi riconoscono una significativa discrezionalità alle autorità di vigilanza[92]. In particolare, il Regolamento IA (cfr. art. 99, par. 7)[93], similmente al sistema GDPR (cfr. art. 83, par. 2) prevede che l'autorità di vigilanza, sia ai fini dell'*an* che del *quantum* della sanzione amministrativa, tiene conto di tutte le circostanze del caso concreto; per esempio, sono circostanze rilevanti: la natura, la gravità e la durata della violazione; il numero di persone interessate e il livello del danno da esse subito.

4.1. Ancora sul rapporto GDPR e Regolamento IA. La DPIA *versus* la FRIA: la duplicazione di adempimenti per le amministrazioni

Spostando maggiormente l'attenzione sul principale oggetto dell'indagine, ossia l'impatto sui soggetti pubblici della sommatoria tra i due Regolamenti, una particolare area di interferenza si rintraccia nell'ambito delle valutazioni d'impatto sui

90. *Ivi*, p. 129.

91. La percentuale sarà più o meno alta a seconda della gravità della violazione attuata. Cfr. art. 99 del Regolamento IA che prevede che la «non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35.000.000 EUR o, se l'autore del reato è un'impresa, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. La non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15.000.000 EUR o, se l'autore del reato è un'impresa, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente».

92. L'Autorità di vigilanza in materia di IA, come si vedrà nel prosieguo, nell'ambito dell'ultimo paragrafo, non coincide con l'Autorità in materia di privacy, il Garante per la protezione dei dati personali.

93. Art. 99, par. 7, *AI Act* prevede che: «(n)el decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e, se del caso, si tiene in considerazione quanto segue: a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA, nonché, ove opportuno, il numero di persone interessate e il livello del danno da esse subito; b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione; c) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento; d) le dimensioni, il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione; e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione; f) il grado di cooperazione con le autorità nazionali competenti al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) il grado di responsabilità dell'operatore tenendo conto delle misure tecniche e organizzative attuate; h) il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore; il carattere doloso o colposo della violazione; j) l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate». Cfr. considerando 168 Regolamento IA laddove prevede che nel valutare «l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up».

diritti fondamentali. Come detto, il Regolamento IA[94] impone al soggetto pubblico o al privato che fornisca servizi pubblici[95] di effettuare tale valutazione di impatto sui diritti fondamentali (c.d. FRIA) quando ci si avvalga di sistemi di IA classificati come ad alto rischio. Allo stesso tempo, l'art. 35 GDPR[96] prevede che quando il trattamento di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, soprattutto allorquando il rischio sia connesso all'uso di nuovo tecnologia, è obbligatorio effettuare la valutazione di impatto dei diritti fondamentali (in inglese *Data Protection Impact Assessment*, in breve DPIA).

Per comprendere se un trattamento di dati personali presenti, nel concreto, un rischio elevato, il titolare del trattamento deve considerare non solo il GDPR ma anche le Linee guida del Gruppo 29[97] nonché i provvedimenti delle Autorità di controllo nazionali.

Tra i trattamenti, che necessitano della DPIA, individuati dal Gruppo 29 vi sono: (i) trattamenti valutativi o di *scoring*, compresa la profilazione; (ii) decisioni automatizzate che producono significativi effetti giuridici (es.: assunzioni, concessione di prestiti, stipula di assicurazioni); (iii) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es.: riconoscimento facciale etc.).

È evidente, dunque, che vi sia un'area di applicazione congiunta degli obblighi di effettuare la DPIA e la FRIA allorquando la pubblica amministrazione si avvalga di intelligenze artificiali ad alto rischio, le quali, *ex se*, rientrano facilmente in una delle categorie di trattamento individuate dal Gruppo 29 e, in particolare, nella più generale ipotesi di «utilizzi innovativi o applicazione di nuove soluzione tecnologiche o organizzative».

In questi casi, l'amministrazione dovrà effettuare, congiuntamente, le due valutazioni, sia la DPIA che la FRIA (come ha evidenziato la dottrina «in particolare, tali sistemi ad alto rischio saranno valutati prima di essere messi sul mercato e durante tutto il loro ciclo di vita (trattasi di una valutazione d'impatto sui diritti fondamentali che si affiancherà alla valutazione di impatto privacy – DPIA – prevista dal GDPR»[98]).

5. Osservazioni conclusive: le problematiche sottese all'applicazione congiunta dei due regolamenti. Il rischio di eccesso di regolazione della tecnologia per il settore pubblico

Come si è anticipato, l'intelligenza artificiale si "nutre" di dati personali e, dunque, le relative discipline sono e devono essere studiate in stretta correlazione.

Non sorprende, pertanto, che il Regolamento sulle intelligenze artificiali e il GDPR dovranno, per forza di cose, trovare applicazione "in modo congiunto". La complementarità tra le discipline

94. Cfr. art. 27: «Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti: a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo».

95. Nonché per operatori che erogano servizi bancari e assicurativi per alcuni sistemi.

96. Cfr. art. 35 GDPR.

97. Cfr. Article 29 Data Protection Working Party 2017.

98. El Sabi 2023, p. 789.

emerge immediatamente dalla lettura dello stesso Regolamento IA, che contiene massicci richiami – sia diretti che indiretti – al GDPR, nonché dalla relazione esplicativa di accompagnamento predisposta dalla Commissione europea, laddove si esplicita che l'applicazione del primo non può pregiudicare l'applicazione del secondo.

Le due discipline sono, per molti versi, simili: la centralità dei diritti fondamentali; la tendenza all'extraterritorialità nonché, *last but not least*, l'approccio regolatorio basato sul rischio.

Tuttavia, dalla comparazione tra le due fonti, emergono molteplici profili di divergenza, tra cui: (i) il difficile rapporto tra alcuni principi fondamentali in materia di GDPR (limitazione delle finalità e minimizzazione dei dati) e (ii) il meccanismo di funzionamento delle intelligenze artificiali che necessitano, per funzionare bene, di grandi quantità di dati.

Ancora, si è evidenziata una distanza per quanto concerne le modalità di qualificazione dei rischi: il GDPR decentralizza la valutazione del rischio sotteso al trattamento, delegando la stessa ai soggetti direttamente coinvolti in base al principio di accountability, l'*AI Act* introduce una valutazione generale e a monte, creando una categorizzazione astratta delle intelligenze artificiali a seconda dei livelli di rischio.

Orbene, alla luce di ciò, un primo problema che si pone è quello di comprendere quale sia il criterio ermeneutico per risolvere i contrasti tra le due fonti. Difatti, non si potrà ricorrere al criterio di specialità, affermando una prevalenza dell'*AI Act* in quanto *lex specialis* rispetto al GDPR, *lex generali*. Ciò perché, innanzitutto, si dubita fortemente sia configurabile, effettivamente, un rapporto di specialità in senso tecnico tra il Regolamento IA e il GDPR. In aggiunta a ciò, il criterio della specialità è inservibile anche in considerazione del fatto che il GDPR tutela un diritto umano fondamentale previsto da una fonte primaria dell'Unione europea[99] e, quindi, ammettere la prevalenza per specialità dell'*AI Act* si porrebbe in contraddizione con il criterio gerarchico.

Oltre al rischio di antinomia tra le norme delle due fonti, la coesistenza delle stesse solleva un'ulteriore problematicità: il tema della duplicazione degli oneri. Difatti, non si può negare che il Regolamento IA contribuisca ad aumentare gli obblighi, in capo agli operatori, e tali obblighi, di sovente, non sostituiscono ma si aggiungono a quelli già contenuti nel GDPR, con conseguente rischio di eccesso regolatorio[100].

Il rischio di eccesso regolatorio di tali materie coinvolge soprattutto l'azione pubblica[101] (si veda l'esempio, trattato al paragrafo che precede, della FRIA, prevista nell'ambito IA, e della DPIA, imposta dal GDPR).

Il crescere degli obblighi ha un impatto ancor più gravoso sul settore pubblico in quanto nel predetto ambito la disciplina delle attività è già *ex se* penetrante e massiccia: le regole sulle IA e privacy devono confrontarsi con ulteriori, certamente non ancillari, norme e principi, tra cui, *in primis*, i principi del procedimento amministrativo, come legalità e trasparenza.

Il quadro regolatorio appare, dunque, per le pubbliche amministrazioni abbastanza saturo e poco coordinato. La tecnologia dovrebbe velocizzare e migliorare la qualità dell'attività amministrativa, *ex* art. 97 Cost., come più volte ricordato dal Consiglio di Stato[102], e, il costante "dubbio giuridico", spesso alimentato dalla ipertrofia normativa, certamente non aiuta ad accelerare il procedimento.

Tutto ciò potrebbe condurre l'amministrazione ad evitare l'utilizzo delle tecnologie più avanzate alla luce della confusione di non essere totalmente *compliant*, evitando così, in radice, di correre il rischio di rispondere per eventuali danni; il timore è "giustificabile" se si considera che le violazioni in materia, oltre ad essere sanzionate dalle Autorità di

99. Cfr. Falletta–Marsano 2024, p. 127.

100. *Ibidem*: «considerati gli ampi margini di potenziale sovrapposizione, l'attuazione delle due discipline, potrebbe portare ad un eccesso di regolamentazione».

101. Probabilmente, il fatto di prevedere questo obbligo, la FRIA, soltanto in capo ai *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), si basa su una presunzione di un rischio specifico in termini di impatto sui diritti fondamentali sotteso alla qualifica.

102. Cfr. nota 88.

vigilanza, possono rientrare nell'ambito di ipotesi di responsabilità amministrativa.

Peraltro, con l'avvento del Regolamento IA, si raddoppiano anche i rischi sanzionatori per le amministrazioni. Come si è visto, sul piano dell'impianto sanzionatorio, il Regolamento IA e il GDPR condividono una impostazione molto simile in quanto la sanzione è determinata mediante una percentuale del fatturato[103] del soggetto destinatario della sanzione. Inoltre, entrambi i sistemi riconoscono una grande discrezionalità alle autorità di vigilanza[104].

Sul punto, è bene rilevare che in Italia, le designate autorità di vigilanza in materia di intelligenza artificiale non coincidono con l'Autorità che si occupa della privacy, il Garante per la protezione dei dati personali. L'Italia ha, infatti, deciso di non attribuire al Garante anche tali competenze, designando, invece, l'AgID (Agenzia per l'Italia Digitale) e l'Agenzia per la Cybersicurezza Nazionale. Tale scelta, sebbene sia comprensibile per certi versi, non volendosi concentrare probabilmente troppe competenze in seno ad un medesimo organo, aumenta il grado di complessità generale sia a valle, sotto il citato profilo sanzionatorio, sia a monte, in quanto enfatizza il rischio di disarmonia – sotto il profilo applicativo – dei due regolamenti[105].

Quindi, anche sotto tale profilo, l'amministrazione che utilizza intelligenze artificiali e nel farlo, nella quasi totalità dei casi, tratta dei dati personali, dovrà confrontarsi non solo con due normative complementari ma anche con più Autorità di vigilanza e con le relative Linee Guida emesse ed *emettende*, con raddoppio dei rischi sanzionatori[106].

103. La percentuale sarà più o meno alta a seconda della gravità della violazione attuata. Cfr art. 99 *AI Act* e 83 e ss. GDPR.

104. Si legge, nel considerando 168 Regolamento IA, che nel valutare «l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up».

105. Si veda la Segnalazione del Garante per la protezione dei dati personali al Parlamento del 25 marzo 2024, ove si evidenziano le ragioni per cui il Garante sarebbe stata l'Autorità di vigilanza più adatta anche ai fini dell'applicazione del Regolamento IA. Nella segnalazione viene evidenziato che: «in ragione della stretta interrelazione tra i.a. e protezione dati, della competenza già acquisita in materia dalle Autorità di protezione dati sul processo decisionale automatizzato (art. 22 del Regolamento UE 2016/679) e delle caratteristiche d'indipendenza che ne connotano lo statuto, sarebbe utile ragionare sulla soluzione proposta dal Comitato europeo per la protezione dati e dal Garante europeo. Con il parere congiunto n. 5 del 2021, essi hanno infatti suggerito l'individuazione, nelle Autorità di protezione dati, delle autorità di controllo per l'i.a. Va, infatti, preliminarmente considerato che il Regolamento obbliga espressamente alla designazione delle Autorità di protezione dati quali autorità competenti rispetto all'applicazione di alcune sue disposizioni. Ai sensi dell'art. 74, p. 8, infatti, "per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III, punti 6, 7 e 8, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680". Inoltre, rispetto all'identificazione biometrica nell'ambito di attività di contrasto si prevede un vaglio autorizzatorio da parte di autorità giudiziarie o amministrative indipendenti (art. 5, p. 3) tenute a verificare l'osservanza, tra l'altro, dei vincoli imposti dalla disciplina di protezione dati. Ciò implica, dunque, l'opportunità dell'attribuzione al Garante anche di tale funzione, in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza. Le Autorità di protezione dati sono, dunque, le uniche autorità effettivamente destinatarie di una riserva di competenza sancita dal Regolamento (cfr., appunto, art. 74, p. 8 oltre alle varie clausole di salvaguardia in favore della protezione dati previste) e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori delicati come quello delle attività di contrasto (art. 5, p. 3). Per tale ragione, sarebbe opportuno attribuire al Garante le funzioni di cui all'art. 70 del Regolamento, ferme restando ovviamente le competenze del Governo in ordine alla generale promozione e regolazione secondaria della materia».

106. Peraltro, muovendo dall'esperienza in tema di DPIA e considerata la sua potenziale sovrapposizione con la FRIA, si consideri che sono molteplici le sanzioni ricevute, negli ultimi anni, da enti pubblici: si può citare

Tuttavia, a mitigare la sommatoria del rischio sanzionatorio concorre l'art. 99, par. 7, lett. c) del Regolamento IA che riconosce, ai fini della determinazione della sanzione, la circostanza della previa comminazione di altra sanzione amministrativa da diversa autorità, più precisamente «se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento».

Riferimenti bibliografici

M. Allena, S. Vernile (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, in Pajno A., Donati F., Perrucci A. (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. 1, il Mulino, 2022

Article 29 Data Protection Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 2017

C. Barett (2019), *Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?*, in "The Sci Tech Lawyer, Chicago", vol. 15, 2019, n. 3

S. Barocas, A.D. Selbst (2016), *Big Data's Disparate Impact*, in "California Law Review", vol. 104, 2016, n. 3

M. Betzu (2021), *I poteri privati nella società digitale: oligopoli e antitrust,* in "Diritto pubblico", 2021, n. 3

F. Bignami (2018), *Introduction. A New Field: Comparative Law and Regulation*, in "GWU Legal Studies working papers", 2018, n. 49

L. Bolognini, E. Pelino (2024), *Codice della disciplina privacy*, Giuffrè, 2024

S. Calzolaio (2023), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

E. Carloni (2020), *I principi della legalità algoritmica. le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2

R. Cantone, E. Carloni (2018), *Corruzione e anticorruzione. Dieci lezioni*, Feltrinelli, 2018

F. Cardarelli (2021), *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro, R. D'Orazio, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

G. Carullo (2024), *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in "CERIDAP", 2024, n. 3

G. Carullo (2020), *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2020, n. 1-2

G. Carullo (2017), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2017

G. Cerrina Feroni (2023), *IA nei processi decisionali della PA, il faro è la Costituzione*, in "Agenda Digitale", 29 maggio 2023

il caso dell'azienda ospedaliera di Perugia, che è stata destinataria del provvedimento sanzionatorio n. 134 del 7 aprile del 2022 del Garante della Protezione dei dati personali per violazione *ex* art. 35 del GDPR.

G. Corasaniti (2022), *Regolazione, autoregolazione, sovraregolazione della rete: dal "far" web al "fair" web*, in "Gli atti digitali di «Gli Stati Generali del Diritto di Internet»", Luiss 1, 2, 3 dicembre 2022

S. D'Ancona (2018), *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2018, n. 3-4

L. D'Avack (2023), *Intelligenza artificiale e diritto: problematiche etiche e giuridiche*, in "Diritto di famiglia e delle persone", 2023, n. 4

S. Davies (2016), *The Data Protection Regulation: A Triumph of Pragmatism over Principle*, in "European Data Protection Law Review", vol. 2, 2016, n. 3

G. De Gregorio, F. Paolucci, O. Pollicino (2021), *L'intelligenza artificiale made in UE è davvero "umano-centrica"? I conflitti della proposta*, in "Agenda Digitale", 22 luglio 2021

S. El Sabi (2023), *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in "Il Diritto dell'informazione e dell'informatica", vol. 39, 2023, n. 4-5

A. Esposito (2023), *Le prime regole degli USA sull'IA: l'impatto dell'Executive Order di Biden*, in "Agenda digitale", 31 ottobre 2023

P. Falletta, A. Marsano (2024), *Intelligenza artificiale e protezione dei dati personali: il rapporto tra il Regolamento sull'intelligenza artificiale e il GDPR*, in "Rivista italiana di informatica e diritto", 2024, n. 1

C.F. Ferrari, G. Morbidelli (2023), *Codice dei contratti pubblici, commentato articolo per articolo*, La Tribuna, 2023

L. Floridi (2021), *The European Legislation on AI: Brief Analysis of its Philosophical Approach*, in "Philosophy & Technology", vol. 34, 2021

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Università degli Studi di Trento, 2023

F. Francario (2021), *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse*, in "Giustiziainsieme.it", 2021

C.G. Granmar (2021), *Global applicability of the GDPR in context*, in "International Data Privacy Law", vol. 11, 2021, n. 3

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", vol. 54, 2021, n. 209

R. Martinez (2019), *Artificial intelligence: Distinguishing between types & definitions*, in "Nevada Law Journal", vol. 19, 2019, n. 3

R. Medaglia, J.R. Gil-Garcia, T.A. Pardo (2023), *Artificial Intelligence in Government: Taking Stock and Moving Forward*, in "Social Science Computer Review", vol. 41, 2023, n. 1

R. Mühlhoff, H. Ruschemeier (2024), *Updating Purpose Limitation for AI: A normative approach from law and philosophy*, 2024

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3

T. Odelberg (2024), *Understanding the Future of Artificial Intelligence Governance: Comparing the EU AI Act and U.S. Executive Order on Safe AI,* in "Ford School of Public Policy", 2024

D. Pager, H. Sheperd (2008), *The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets*, in "Annual Review of Sociology", vol. 34, 2008

A. Police (2024), *Principi e azione amministrativa*, in F.G. Scoca (a cura di), "Diritto Amministrativo", Giuffrè, 2014

O. Pollicino (2023), *Washington effect o Bruxelles effect? Regolamentazioni dell'IA a confronto*, in "formiche", 31 ottobre 2023

O. Pollicino (2019), *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

J.A. Powell (2008), *Structural Racism: Building upon the Insights of John Calmore*, in "North Carolina Law Review", vol. 86, 2008, n. 3

A. Puckzo (2024), *An Ambiguous Relationship between Public Administration and AI*, in P. Yao Lartey (ed.), "Recent Advances in Public Sector Management", IntechOpen, 2024

G. Resta (2022), *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale?*, in "Il Diritto dell'Informazione e dell'Informatica", 2022, n. 2

A. Simoncini, S. Suweis (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1

D. Solove, P.M. Schwarts (2022), *ALI Data Privacy: Overview and Black Letter Text*, in "UCLA Law Review," vol. 68, 2022, n. 5

L. Torchia (2024), *Poteri pubblici e poteri privati nel mondo digitale*, in "Il Mulino", 2024, n. 1

S. Trozzi (2024), *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, in "federalismi.it", 2024, n. 1

P. Wang (2019), *On Defining Artificial Intelligence*, in "Journal of artificial general intelligence", vol. 10, 2019, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0211 • articolo sottoposto a peer review • pubblicato in anteprima il 25 feb. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Enza Cirone

Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative

Il contributo esplora l'evoluzione dell'approccio normativo dell'Unione europea nel rispondere alle sfide poste dalle tecnologie emergenti, evidenziando la transizione da un modello basato sulla neutralità tecnologica a strumenti innovativi e flessibili, come gli spazi di sperimentazione normativa (c.d. *regulatory sandboxes*). Questi strumenti, centrali nel quadro dell'AI Act, sono concepiti come veri e propri laboratori di regolamentazione, permettendo di valutare l'efficacia delle norme esistenti e di apportare modifiche mirate per rispondere a esigenze tecniche e sociali in continua evoluzione. Nonostante le opportunità offerte, emergono alcune criticità che richiedono attenzione. Questioni legate alla trasparenza, all'equità di accesso e alla distribuzione delle responsabilità tra innovatori, autorità pubbliche e società civile sollevano importanti interrogativi. Per evitare frammentazioni normative tra gli Stati membri e mitigare i rischi di "cattura regolatoria", è fondamentale definire criteri di selezione e meccanismi di supervisione chiari e uniformi. Questo contributo intende mettere in luce come le *sandboxes* normative, se implementate correttamente, possano divenire strumenti strategici per una regolazione basata su evidenze empiriche, favorendo un dialogo costruttivo tra regolatori e innovatori. In linea con i principi di trasparenza e inclusività sanciti dall'Unione europea, esse rappresentano una nuova frontiera per un modello di governance capace di affrontare le complessità delle tecnologie emergenti.

Spazi di sperimentazione normativa – Regulatory sandboxes – Unione europea – Co-regolazione Intelligenza artificiale

Regulatory sandboxes in the European Union: Regulating innovation between principles and practical applications

This contribution examines the evolution of the EU's regulatory approach in addressing the challenges posed by emerging technologies, highlighting the transition from a technology-neutral model to innovative and flexible tools such as regulatory sandboxes. These instruments, central to the framework of the AI Act, are designed as actual regulatory laboratories, enabling the assessment of existing rules and the implementation of targeted modifications to address evolving technical and social needs. Despite the opportunities they offer, specific critical issues demand attention. Concerns about transparency, equitable access, and the allocation of responsibilities among innovators, public authorities, and civil society raise significant questions. Establishing clear and uniform selection criteria and oversight mechanisms is essential to prevent regulatory fragmentation among Member States and mitigate the risks of regulatory capture. This contribution seeks to shed light on how regulatory sandboxes, if properly implemented, can become strategic tools for evidence-based regulation, fostering constructive dialogue between regulators and innovators. Aligned with the principles of transparency and inclusivity enshrined in the European Union, they represent a new frontier for a governance model capable of addressing the complexities of emerging technologies.

Regulatory sandboxes – European Union – Coregulation – Artificial intelligence

L'Autrice è assegnista di ricerca in Diritto dell'Unione europea presso l'Università degli studi di Firenze

Sommario: 1. Dalla neutralità tecnologica agli spazi di sperimentazione normativa: l'evoluzione dell'approccio regolatorio. – 2. Spazi di sperimentazione normativa: principi teorici e prassi applicative in alcuni contesti nazionali. – 2.1. Il contributo del Regolamento sull'intelligenza artificiale. – 3. Sperimentando si impara (…e si innova)? – 3.1. Quali sfide nell'implementazione delle *regulatory sandboxes*? – 4. La (necessaria) sinergia tra pubblico e privato negli spazi di sperimentazione normativa. – 5. Osservazioni conclusive.

"Costruire teorie prima di aver raccolto i fatti
è un errore madornale: conduce ad adattare i fatti alle teorie,
invece che adattare le teorie ai fatti".

Arthur Conan Doyle, *La valle della paura,* 1914

1. Dalla neutralità tecnologica agli spazi di sperimentazione normativa: l'evoluzione dell'approccio regolatorio[1]

Negli ultimi decenni, il rapido avanzamento dell'innovazione e della tecnologia ha profondamente trasformato vari aspetti della società, sollevando quesiti sull'efficacia e adeguatezza del quadro normativo esistente nel rispondere alle nuove sfide[2] e nel coordinare i diversi approcci regolatori tra giurisdizioni nazionali[3].

La regolamentazione di tecnologie spesso dirompenti, come l'intelligenza artificiale e la *blockchain*, solleva criticità significative legate alla loro natura dinamica e in continua evoluzione, che contrasta con l'approccio tradizionale alla legislazione, generalmente poco adeguato ad adattarsi rapidamente ai cambiamenti. A complicare ulteriormente la questione vi è l'opacità tecnologica[4], ossia la difficoltà di comprendere a fondo il funzionamento di sistemi tecnologici complessi. Questa caratteristica evidenzia la necessità di coinvolgere esperti con competenze specifiche nella stesura di normative che siano, allo stesso tempo, esaustive e in grado di garantire certezza giuridica.

Negli ultimi tempi, l'interazione tra tecnologia e diritto si è manifestata (e continua a manifestarsi) in tutte le sue multiformi sfaccettature. Se, da un lato, l'innovazione tecnologica può richiedere

1. Il presente scritto costituisce una rielaborazione della relazione tenutasi in occasione del convegno "Intelligenza artificiale, dati e diritto", organizzato dal centro di eccellenza DIIS dell'Università di Cagliari, 12-13 dicembre 2024. L'autrice desidera ringraziare i proff. Andrea Deffenu e Daniele Amoroso per l'organizzazione del convegno, nonché i proff. Corrado Chessa e Federico Cappai per gli utili commenti a valle della relazione. Un sentito ringraziamento va inoltre ai revisori anonimi e alla prof.ssa Adelina Adinolfi per i preziosi suggerimenti. Ogni eventuale errore, omissione o inesattezza è da attribuirsi esclusivamente all'autrice.
2. Per una disamina degli approcci adottati dall'Unione europea per migliorare il processo decisionale a lungo termine e la capacità di risposta alle sfide future, v. Umbach 2024.
3. La regolazione è talvolta considerata nell'ottica di mitigazione dei rischi: "[regulation is an] organized attempt to manage risks or behaviour in order to address a collective problem or concern", Yeung 2017, p 11.
4. Vaassen 2022; Chesterman 2021; Surden–Williams 2016, p. 121 ss.

cambiamenti nei sistemi giuridici tradizionali[5], dall'altro, ciò non implica necessariamente (e, in ogni caso, non dovrebbe implicare) uno smantellamento dell'assetto fondato sui principi essenziali dello Stato di diritto[6].

La regolamentazione di ambiti fortemente influenzati dall'innovazione tecnologica richiede un equilibrio delicato tra la promozione dell'innovazione e la tutela degli interessi coinvolti, imponendo ai legislatori decisioni complesse: stabilire se intervenire, quale approccio normativo adottare, quali parti interessate coinvolgere, definire la durata della validità delle norme e valutare la necessità di modificare o abrogare normative già esistenti.

Di fronte a queste difficoltà, l'evoluzione tecnologica[7] ha spinto il legislatore dell'Unione ad adottare un approccio normativo più flessibile[8], orientato a rispondere alle esigenze degli operatori senza imporre soluzioni specifiche. Per evitare di favorire alcune innovazioni a scapito di altre, è stato introdotto il principio di neutralità tecnologica e dei modelli di business, che garantisce a utenti e organizzazioni la libertà di scegliere le tecnologie da utilizzare, senza "interferenze" normative.

Questo approccio presenta sfide su due livelli. Da un lato, i regolatori devono elaborare normative che non privilegino determinate tecnologie o modelli di business, assicurandosi che le norme siano applicabili in modo equo. Ciò richiede una definizione precisa dell'ambito di applicazione, per evitare discriminazioni verso tecnologie simili per base tecnica e assicurare che le regole siano neutrali rispetto al tipo di tecnologia[9]. Dall'altro lato, la neutralità impone agli interpreti del diritto una valutazione caso per caso, per garantire che le norme siano adattate alle caratteristiche specifiche di ogni tecnologia o prodotto[10]. In teoria, questo orientamento amplia la portata delle normative, richiedendo un'analisi flessibile per una corretta applicazione delle regole in contesti tecnologici diversi.

La regolazione delle nuove tecnologie riveste un'importanza cruciale nell'ordinamento giuridico

5. Cfr., *inter alia*, Faralli 2019, pp. 43-52: "per i giuristi si è posto il problema se e come fissare delle regole senza soffocare i progressi della scienza, ma anche senza ledere i diritti degli individui".
6. Greenstein 2022; Buchholtz 2020.
7. Con riferimento all'intelligenza artificiale, Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale nell'era digitale, P9_TA(2022)0140, punto 121.
8. La Commissione, già nei primi anni Duemila, aveva mostrato un crescente interesse verso i cosiddetti metodi alternativi di regolazione. A tal proposito, basti citare il Libro bianco della Commissione sulla Governance europea del 2001 e il successivo Accordo interistituzionale del 2003, che ne ha recepito parzialmente i contenuti. Questi documenti testimoniano una tendenza che, nei vent'anni successivi, si sarebbe consolidata – sebbene non priva di contraddizioni – nell'obiettivo di migliorare sia la qualità della legislazione europea sia le procedure decisionali. Tale percorso si è inserito nel quadro più ampio delle iniziative volte alla razionalizzazione normativa, quali le proposte di "Better Regulation" e "Smart Regulation". V. Commissione europea, "La governance Europea - Un libro bianco", COM(2001) 428; Parlamento europeo, Consiglio, Commissione, "Accordo interistituzionale «Legiferare meglio»", 2003/C 321/01, sostituito dall'Accordo interistituzionale del 13 aprile 2016. Riguardo ai due programmi, v. European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, "A strategic review of better regulation in the European Union", COM(2006) 689; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Second strategic review of Better Regulation in the European Union", COM(2008) 32; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Smart Regulation in the European Union", COM(2010) 543. Cfr. anche Bartoloni 2021.
9. Questo aspetto è chiaramente evidenziato nei *Principi UNIDROIT sui Beni Digitali e sul Diritto Privato*, i quali esprimono preoccupazione su questo fronte.
10. Cfr. European Law Institute 2022: "Principle 3 – Case Specific Approach - In the application of the Principles it should, for each Principle and in each specific case, be considered which type of Blockchain is used and who the parties involved are, and which type of Smart Contract is used, as referred to in Principle 2".

dell'Unione europea, data la necessità di armonizzare il progresso tecnologico con i principi fondamentali e gli obiettivi comuni. Per affrontare queste sfide, la Commissione europea[11] ha adottato un approccio normativo orientato alla flessibilità e alla neutralità, come indicato nella *Better Regulation Toolbox*[12], al fine di rimanere aperti a soluzioni innovative capaci di contribuire al raggiungimento degli obiettivi politici di ciascuna misura.

Non è la prima volta che nell'ordinamento dell'Unione viene adottato il principio di neutralità tecnologica. Un esempio significativo è rappresentato dal Regolamento generale sulla protezione dei dati, dove al considerando 15[13] viene sottolineato che le misure di tutela dei dati personali si applicano indipendentemente dalla tecnologia utilizzata. Questo dimostra come l'approccio neutrale rispetto alla tecnologia miri ad ampliare la portata della normativa, piuttosto che limitarla.

La neutralità tecnologica si configura quindi come uno strumento per evitare il rischio di elusione degli obiettivi della normativa[14], basandosi sul principio di equivalenza tra realtà online e offline, oltre a rappresentare un mezzo efficace per ridurre il rischio che le normative diventino rapidamente obsolete a causa dall'evoluzione tecnologica.

Di recente, stanno emergendo approcci regolatori che, invece di cercare di prevedere tutti i possibili cambiamenti[15], facilitano l'adattamento delle politiche in risposta a nuovi sviluppi. Tra questi strumenti figurano le clausole sperimentali, le c.d. *sandboxes* regolatorie e le politiche temporanee[16]. Essendo tecnologicamente neutrali, questi strumenti permettono di valutare e gestire i rischi senza dipendere dagli assetti – tecnologici e non – previsti dalla normativa. Nel loro complesso, questi strumenti sono anche conosciuti come "spazi di sperimentazione normativa".

Nonostante recenti previsioni normative in tale direzione, questi strumenti innovativi non sono ancora ampiamente diffusi nell'ordinamento giuridico dell'Unione, e le iniziative legislative che introducono differenziazioni giuridiche temporanee rimangono sporadiche. Un esempio significativo più risalente è rappresentato dalla Direttiva del Consiglio 1999/85[17], che ha modificato la Direttiva 77/388 per consentire, in via sperimentale, l'applicazione di un'aliquota IVA ridotta per i servizi ad alta intensità di manodopera. Questo intervento mirava a stimolare l'occupazione e contrastare l'economia sommersa, prevedendo una durata limitata, la partecipazione di nove Stati membri e una successiva valutazione dei risultati.

11. L'*Expert Group on Regulatory Obstacles to Financial Innovation* (ROFIEG) della Commissione europea aveva già inserito tra le sue raccomandazioni quella di valutare l'opportunità di istituire una "sandbox normativa" a livello di Ue proprio al fine di migliorare gli effetti dell'innovazione tecnologica, Expert Group on Regulatory Obstacles to Financial Innovation 2019, p. 71 ss.
12. European Commission 2023, p. 176.
13. "Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine", Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
14. Hildebrandt–Tielemans 2019.
15. Alcuni autori, tuttavia, sostengono criticamente che sia impraticabile disciplinare in modo esaustivo il futuro, Garben 2020, p. 93.
16. de Boer 2018; Ranchordás–van't Schip 2020.
17. Direttiva 1999/85/CE del Consiglio del 22 ottobre 1999 che modifica la direttiva 77/388/CEE, con riguardo alla possibilità di introdurre a titolo sperimentale un'aliquota IVA ridotta sui servizi ad alta intensità di lavoro. La direttiva è stata abrogata dalla Direttiva 2006/112/CE del Consiglio del 28 novembre 2006 relativa al sistema comune d'imposta sul valore aggiunto.

Tuttavia, negli ultimi anni si registra una crescente apertura verso l'adozione di approcci sperimentali. In particolare, il 16 novembre 2020, il Consiglio dell'Unione europea ha adottato le Conclusioni sulle sandboxes regolatorie e clausole sperimentali[18], riconoscendo tali strumenti come un mezzo strategico per sostenere un quadro normativo flessibile, resiliente e orientato all'innovazione. Le Conclusioni sottolineano come le *sandboxes* regolatorie possano rappresentare una leva significativa per incentivare l'innovazione e la crescita in diversi settori, con un impatto particolarmente positivo per le PMI, incluse le microimprese e le start-up.

Inoltre, in linea con il "principio di innovazione" – volto a garantire che le normative si adattino all'evoluzione tecnologica – nelle Conclusioni il Consiglio ha incoraggiato la Commissione a valutare l'introduzione di clausole sperimentali caso per caso durante la redazione e revisione delle normative[19]. Ha anche suggerito di considerare l'utilizzo di queste clausole nelle verifiche *ex post* e nei controlli di idoneità, basandosi su uno scambio di informazioni con gli Stati membri.

La comunicazione della Commissione europea "Una nuova agenda europea per l'innovazione" ha, infatti, indicato la creazione di "condizioni quadro per l'innovazione tecnologica avanzata", che include approcci sperimentali alla regolamentazione, tra cui le *sandboxes* normative, come uno dei pilastri di questa agenda. Questo orientamento si è concretizzato in iniziative come le "strutture di prova e sperimentazione" del Programma Europa Digitale 2021–2027[20] e nel regime pilota dell'Ue per la tecnologia a registro distribuito[21].

Un altro strumento rilevante a livello europeo è la già citata *Better Regulation Toolbox*, che ha integrato alcune delle indicazioni del Consiglio sull'uso della sperimentazione normativa. Questo *Toolbox*, ideato per incentivare la ricerca e l'innovazione, riconosce le "clausole sperimentali" come meccanismi utili per una regolamentazione flessibile e aperta al progresso. Secondo questo documento, tali clausole possono risultare efficaci quando è necessario specificare dettagli tecnici di un prodotto o tecnologia, lasciando aperta la possibilità di raggiungere l'obiettivo politico anche attraverso soluzioni innovative future.

Tuttavia, il *Toolbox* tende a definire le *sandboxes* regolatorie in modo riduttivo, descrivendole come "quadri sperimentali sofisticati"[22] o strumenti "che permettono di testare innovazioni in ambienti reali, con garanzie e supporto regolamentare"[23].

In realtà, come si cercherà di dimostrare in questo contributo, le *regulatory sandboxes* rappresentano molto più di semplici clausole sperimentali: si configurano come strumenti di co-regolazione, caratterizzati dall'applicazione di misure ad hoc per casi specifici e da una fase di monitoraggio continuo. In particolare, si ritiene che gli spazi di sperimentazione normativa possano favorire la creazione di normative basate su evidenze tecniche specifiche, evitando formulazioni generiche e garantendo una valutazione e un aggiornamento costante della normativa.

18. Consiglio dell'Unione europea 2020.
19. A tal fine, nel 2021 la Presidenza Slovena ha inviato agli Stati membri un questionario e documenti di policy per monitorare le tipologie di *sandbox* esistenti e raccogliere le migliori pratiche. I documenti sottoposti agli Stati per la consultazione sono: a) The role of sandboxes in promoting flexibility and innovation in the digital age; b) ESAs Joint Committee report FinTech: Regulatory sandboxes and innovation hubs, January 2019; c) UNSGSA FinTech Working Group and CCAF 2019, Early Lessons on Regulatory Innovations to Enable Inclusive FinTech; d) Regulatory Sandboxes and Innovation Hubs for Fintech; e) Regulatory sandboxes and financial inclusion.
20. Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.
21. Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE.
22. Traduzione dell'A., Cfr. European Commission 2023, p. 178.
23. Traduzione dell'A., *ibidem*.

Ciononostante, come rilevato da alcuni autori[24], questi strumenti possono comportare dei rischi, poiché lasciano margine agli innovatori per sottrarsi alle proprie responsabilità sia durante la fase di sperimentazione che in seguito, esponendo i partecipanti a potenziali pericoli.

Alla luce di quanto precede, il contributo si propone di indagare le tensioni giuridiche che emergono nell'ambito degli spazi di sperimentazione normativa, con particolare attenzione ai principi di legalità e parità di trattamento. Queste tensioni si collocano al confine tra la promozione dell'innovazione e la necessità di garantire la sicurezza, imponendo una riflessione approfondita sul bilanciamento tra esigenze spesso contrapposte.

Il lavoro si articola in tre parti. In primo luogo, si procederà a una disamina dei fondamenti teorici e delle principali prassi applicative osservate in contesti nazionali selezionati, con uno specifico focus sul recente Regolamento (UE) 2024/1689[25] (d'ora in avanti AI Act). Questa analisi permetterà di chiarire i contorni giuridici e operativi degli spazi di sperimentazione normativa nel quadro dell'ordinamento europeo. Successivamente, il contributo valuterà se tali strumenti possano effettivamente rappresentare un mezzo efficace per favorire l'innovazione, esaminando al contempo gli ostacoli che potrebbero emergere rispetto ai principi fondamentali del diritto dell'Unione. Si considereranno, in particolare, le sfide legate alla trasparenza, all'equità di accesso e alla conformità ai valori democratici. Infine, si analizzerà il ruolo degli spazi di sperimentazione normativa nel contesto della coregolazione, evidenziando come la necessaria sinergia tra regolatori e innovatori possa contribuire a modellare un quadro regolatorio più dinamico e resiliente.

2. Spazi di sperimentazione normativa: principi teorici e prassi applicative in alcuni contesti nazionali

Prima di esaminarne i fondamenti teorici e le prassi applicative, è necessario definire gli spazi di sperimentazione normativa e le *regulatory sandboxes*[26], chiarendo in primis se vi siano differenze concettuali tra i due.

Sebbene la letteratura giuridica[27], i documenti di policy[28] e le normative[29] offrano una varietà di definizioni, non esiste una versione che si possa ritenere generalmente accettata, poiché, come sostenuto in dottrina[30], questi concetti variano in base al contesto giuridico nazionale e all'interpretazione che ne viene fornita.

Ai fini del presente contributo, la definizione adottata è quella accolta dal Consiglio dell'Unione europea che intende gli spazi di sperimentazione normativa come "quadri concreti che, fornendo un contesto strutturato per la sperimentazione, consentono, se del caso in un ambiente reale, di testare tecnologie, prodotti, servizi o approcci innovativi – al momento soprattutto nel contesto della digitalizzazione – per un periodo di tempo limitato e

24. "[…] [T]oo often sandboxes are misunderstood, misused, or mismanaged. Regulatory agencies should use sandboxes to keep up to date with fast-paced innovation and promote market competition without sacrificing consumer protection. Real innovation-minded regulatory agencies see sandboxes as means, not ends", Quan 2019.
25. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
26. Il termine deriva dall'informatica dove con *sandbox* si intende uno strumento atto a testare un determinato sistema. Yordanova 2019.
27. V. *ex multis*, Allen 2020; Allen 2019; Zetzsche–Buckley–Barberis–Arner 2017.
28. Commissione europea, "Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia", COM(2020) 65, 19 febbraio 2020; Financial Stability Board 2020; Financial Conduct Authority 2015.
29. Regolamento (UE) 2024/1689, cit.; Regolamento (UE) 2021/694, cit.
30. Zetzsche–Buckley–Barberis–Arner 2017; Knight–Mitchell 2020; Armour–Sako 2020; Ranchordás 2020; Bar-Siman-Tov 2018.

in una parte limitata di un settore o di un ambito soggetto a vigilanza regolamentare, garantendo la messa in atto di opportune misure di salvaguardia"[31]. In altre, parole, si tratta di ambienti, sia virtuali che fisici, concepiti per consentire la sperimentazione temporanea di progetti tecnologicamente innovativi, con la possibilità di applicare deroghe alle normative vigenti nel settore di riferimento. Tali ambienti offrono ai promotori l'opportunità di condurre test in modo approfondito ed efficace. Un ulteriore elemento distintivo consiste nella possibilità di impiegare i risultati delle sperimentazioni come base per future e potenziali modifiche legislative.

Questa definizione così ampia mette in luce le tre principali caratteristiche[32] di questi strumenti: (i) il carattere temporaneo delle misure; (ii) l'approccio regolatorio basato sul metodo del tentativo ed errore e (iii) il coinvolgimento di diversi portatori di interesse.

Va inoltre chiarito che le istituzioni europee utilizzano i termini spazi di sperimentazione normativa e *regulatory sandboxes* in modo intercambiabile[33], considerando quest'ultimo l'equivalente inglese del primo, specialmente nel contesto delle normative sulle tecnologie emergenti, come l'intelligenza artificiale.

Questa scelta terminologica potrebbe riflettere un tentativo di armonizzazione concettuale, finalizzato a rendere accessibili e comprensibili, sia a livello nazionale che europeo, concetti complessi e innovativi. Tale tendenza riflette l'impegno dell'Unione europea a promuovere soluzioni uniformi e condivise, considerando che tali sperimentazioni sono state avviate in maniera autonoma dagli Stati membri e si sono, pertanto, sviluppate con approcci tecnici differenti e in ambiti di applicazione eterogenei. Infatti, sebbene il concetto di *regulatory sandbox* sia relativamente recente, numerose *sandboxes* sono già operative sia a livello europeo sia a livello globale[34]. Poiché questo articolo si propone di analizzare questi strumenti da una prospettiva giuridica piuttosto che tecnica, è opportuno menzionare alcuni esempi rappresentativi scelti da diverse giurisdizioni, ognuno dei quali rappresenta un interessante esempio di implementazione.

Il primo e più diffuso è quello delle *sandboxes* finanziarie o fintech, settore in cui le *sandboxes* normative hanno avuto origine. La prima sandbox è stata lanciata nel 2015 nel Regno Unito per iniziativa della Financial Conduct Authority (FCA)[35], seguita negli anni successivi da numerosi progetti analoghi. Il funzionamento di questa *sandbox* consiste nel fornire un ambiente regolatorio controllato in cui le imprese possono testare prodotti o servizi finanziari innovativi senza essere soggette immediatamente a tutte le normative vigenti. Ogni progetto approvato è monitorato dalla FCA, che fornisce supporto e guida per garantire la conformità, riducendo al minimo i rischi per i consumatori.

In Italia[36], uno strumento simile è stato introdotto con il decreto legge 30 aprile 2019 n. 34, conosciuto come "Decreto Crescita", seguito successivamente dal decreto del Ministero dell'Economia e delle Finanze del 30 aprile 2021, n. 100. La *sandbox* italiana prevede che le imprese che desiderano testare soluzioni innovative presentino una domanda alle autorità competenti, che valutano la proposta e, in caso di approvazione, consentono

31. Consiglio dell'Unione europea 2020, p. 8.
32. Cfr. Ranchordás 2020; Bar-Siman-Tov 2018.
33. In particolare, nelle *Conclusioni* 2020, il Consiglio dell'Unione europea evidenzia come le *regulatory sandboxes* – o spazi di sperimentazione normativa – siano strumenti essenziali per consentire alle imprese di testare soluzioni innovative in un ambiente regolato ma flessibile, dove tali soluzioni non sono immediatamente soggette ai requisiti normativi tradizionali. Allo stesso modo, nella proposta di Regolamento sull'Intelligenza Artificiale e nella versione definitiva pubblicata in Gazzetta Ufficiale, si fa riferimento agli spazi di sperimentazione normativa utilizzando l'espressione inglese *regulatory sandboxes*, sottolineando l'importanza di questi ambienti per favorire un continuo adattamento normativo alle trasformazioni tecnologiche.
34. World Bank Group 2020, p. 5.
35. Financial Conduct Authority 2017.
36. Per un approfondimento sui potenziali conflitti tra le *sandboxes* e il sistema costituzionale italiano, si rimanda a Milanesi 2023.

l'avvio del progetto in un ambiente controllato. Durante la fase di sperimentazione, le imprese sono soggette a requisiti regolatori ridotti, ma devono fornire rapporti periodici sullo stato del progetto e sui risultati ottenuti.

Di particolare interesse è anche il programma "Sperimentazione Italia", regolato dal decreto legge 16 luglio 2020, n. 76, specificamente dall'art. 36, che si innesta nell'ambito della cosiddetta "trasformazione digitale della pubblica amministrazione", in un'ottica multisettoriale. Tale iniziativa è stata applicata in particolare nei progetti di "smart cities" e, nello specifico, nel campo della "smart mobility"[37].

Anche altri Stati membri dell'Ue hanno adottato spazi di sperimentazione normativa. In Spagna, ad esempio, è stata istituita una *sandbox* per il settore fintech, simile a quella italiana[38]. Qualsiasi soggetto interessato a proporre un progetto innovativo per il settore può presentare domanda, purché rispetti requisiti essenziali, quali la dimostrazione di fornire un contributo innovativo al sistema finanziario, la sua "natura fintech" e la sostenibilità del progetto. Il legislatore spagnolo ha dato rilievo sia al progresso tecnologico che alla protezione dei consumatori e alla stabilità dei mercati, prevedendo una adeguata politica finanziaria a contorno dell'iniziativa oltre che tutele per i consumatori e i servizi finanziari[39].

Durante l'intera fase di test, l'Autorità di vigilanza monitora il rispetto delle regole previste dal protocollo e dalla normativa, con possibilità di interrompere la sperimentazione in caso di violazioni. Inoltre, l'Autorità redige una relazione finale che, trasmessa al Comitato di coordinamento, può portare a proposte di modifica legislativa incluse nel rapporto annuale della SGTFI e presentate in Parlamento dal Ministro degli Affari economici[40].

La Germania ha incentivato l'uso di clausole sperimentali in vari settori, tra cui il trasporto intelligente e l'istruzione[41], a livello dei singoli Länder. L'esperienza tedesca in materia di *regulatory sandboxes* si distingue nel contesto europeo per il suo approccio strutturato e coordinato a livello nazionale. Già dal 2018, il Ministero Federale dell'Economia ha pubblicato una guida[42] che illustra il concetto di *sandbox* normativa, i suoi scopi e le modalità di funzionamento, promuovendo l'adozione di deroghe sperimentali da parte delle autorità locali.

Una caratteristica peculiare del modello tedesco è l'impiego di clausole sperimentali che permettono ai governi regionali di autorizzare temporaneamente l'applicazione di norme meno rigide per favorire la sperimentazione di progetti innovativi. Queste clausole sono incorporate nelle disposizioni legislative locali o federali e prevedono la partecipazione di vari enti governativi, garantendo così un elevato grado di flessibilità. Di conseguenza, le tempistiche, i procedimenti e i criteri di approvazione possono variare notevolmente in base alla tipologia di progetto presentato. Tra le iniziative più rilevanti[43] si segnalano quelle nel campo della mobilità intelligente, come

37. Rugani 2024, e dottrina ivi citata.
38. Gomez Santos 2021. Per un'analisi approfondita della legge spagnola v. Trapani 2022 e Zunzunegui 2020.
39. Le candidature possono essere presentate durante finestre semestrali e il processo coinvolge diversi organi, tra cui la Segreteria Generale del Tesoro e della Finanza Internazionale (SGTFI) e altre autorità pubbliche: la Banca di Spagna, la Commissione Nazionale per il Mercato dei Valori, e la Direzione Nazionale per Assicurazioni e Fondi Pensione. Il coordinamento è affidato a un Comitato specifico, mentre la valutazione preliminare dei progetti è svolta dall'Autorità competente, che firma con il proponente un protocollo contenente modalità e termini della sperimentazione in caso di approvazione. Si veda, Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero.
40. Ministerio de Asuntos Economicos y Transformaciòn Digital, *Sandbox Financiero*. Vedi anche Banco de España, *Sandbox: the testing environment for financial innovation*, 2024.
41. Maass 2021; Freund 2003; Horn 1989.
42. Si veda il report *Making space for innovation. The handbook for regulatory sandboxes*, 2019.
43. Per consultare gli altri progetti attivi v. il sito del Ministero.

il progetto avviato ad Amburgo, reso possibile grazie a modifiche legislative specifiche[44].

In virtù di questo approccio, la Germania ha assunto un ruolo di primo piano nello sviluppo di strumenti regolatori innovativi, investendo risorse significative e coinvolgendo attivamente sia il settore pubblico che quello privato. Questo sistema ha garantito ampie opportunità di sperimentazione per i privati, pur mantenendo un controllo sulle potenziali criticità. Va però rilevato che rimane elevata la discrezionalità delle autorità pubbliche nel concedere le autorizzazioni, nell'ottica di incentivare l'innovazione senza alterare in modo permanente il quadro normativo vigente.

In Portogallo, la sperimentazione ha luogo in un'area dedicata, chiamata "Zona Franca Tecnologica", una zona geografica e tematica destinata a progetti innovativi[45].

Un altro importante esempio di spazio di sperimentazione normativa è rappresentato dalla *sandbox* normativa sviluppata dall'Information Commissioner's Office (ICO) del Regno Unito nell'ambito della protezione dei dati[46] con riferimento a tecnologie particolarmente innovative, come la realtà aumentata, oppure tecnologie di riconoscimento biometrico.

Il funzionamento della *sandbox* promossa dall'ICO prevede una fase iniziale di selezione, in cui le organizzazioni presentano le loro proposte innovative. Se accettate, le organizzazioni ricevono supporto continuo e indicazioni specifiche dall'ICO durante la fase di test. Questo approccio permette di individuare e risolvere eventuali problematiche di conformità prima del lancio ufficiale sul mercato.

La richiesta di strumenti di sperimentazione normativa è in aumento anche nel campo sanitario. Come dimostrano studi sistematici condotti in questo ambito, queste iniziative sono concentrate soprattutto nei paesi ad alto reddito[47], dove l'obiettivo individuato è di sostenere l'adozione di nuove tecnologie, in particolare quelle legate alla salute digitale[48]. In tale contesto, guardare a esperienze extraeuropee risulta particolarmente significativo, dato che in molti paesi terzi queste sperimentazioni hanno già trovato applicazione concreta, dimostrando sia le potenzialità di tali strumenti sia l'urgenza per l'Unione europea di sfruttare al meglio queste opportunità, colmando eventuali divari rispetto ai paesi leader nelle tecnologie emergenti.

Un esempio concreto di *sandbox* normativa nel settore sanitario è quello di Singapore, dove il Ministero della Salute ha lanciato nel 2018 il c.d. *Licensing Experimentation and Adaptation Programme* (LEAP)[49]. Questo programma ha creato una *sandbox* dedicata alla telemedicina e alla medicina mobile, con l'obiettivo di comprendere meglio il funzionamento della nuova tecnologia, identificare i rischi potenziali e stabilire misure per mitigarli, prima di procedere con la concessione delle licenze[50], in conformità con il *Singaporean*

44. V. progetto "HEAT" (*Hamburg Eletric Autonomous Transportation*) che consisteva nel testare bus a guida autonoma per le strade di Amburgo. La deroga normativa è contenuta nella Sezione 7(2) della Legge sui Trasporti di Passeggeri che prevede che, per consentire la sperimentazione pratica di nuovi modi o mezzi di trasporto, l'Autorità competente al rilascio delle licenze può, caso per caso e su richiesta, autorizzare delle deroghe alle disposizioni della Legge sui trasporti per un periodo massimo di quattro anni. Si precisa inoltre che tali deroghe non devono porsi in contrasto con gli interessi del trasporto pubblico.

45. Trapani 2022.

46. Information Commissioner's Office, *The Guide to the Sandbox*.

47. Leckenby–Dawoud–Bouvy–Jónsson 2021.

48. A tal riguardo, si tenga in considerazione che la Costituzione francese dà la possibilità di adottare leggi sperimentali, sia a livello nazionale che locale. Cfr. Stahl 2010.

49. Attrey–Lesher–Lomax 2020.

50. Per raggiungere gli obiettivi prefissati, il Ministero della Salute di Singapore ha istituito una piattaforma di cooperazione con i fornitori coinvolti per creare un ambiente sicuro per la telemedicina e la medicina mobile, adottando un approccio basato sulla valutazione del rischio. L'obiettivo finale della *sandbox* normativa era giungere a una regolamentazione completa della telemedicina e della medicina mobile come servizi sanitari autorizzati. Tale obiettivo è stato dichiarato raggiunto a febbraio 2021, portando alla chiusura della *sandbox*.

Healthcare Services Act[51]. Il funzionamento del programma LEAP si basa su una stretta collaborazione tra le autorità e le imprese partecipanti, che devono rispettare criteri di sicurezza rigorosi durante l'intera fase di sperimentazione.

L'esperienza di Singapore, e in particolare la conclusione positiva della *sandbox* normativa avviata nel 2018, dimostra che questi strumenti possono essere applicati con successo anche nel settore sanitario, sebbene alcuni autori abbiano sollevato delle criticità che concernono potenziali rischi per la sicurezza dei pazienti, poca trasparenza e frizioni con alcuni principi etici[52].

In generale, gli esempi citati evidenziano come la questione delle *sandboxes* normative non sia confinata a un solo settore, ma si estenda a molteplici ambiti sociali ed economici, ciascuno con le proprie sfide e opportunità.

2.1. Il contributo del Regolamento sull'intelligenza artificiale

Come già anticipato in apertura, un settore rilevante per l'applicazione delle *sandboxes* normative è quello dell'intelligenza artificiale.

Un esempio interessante a questo proposito è quello della Norvegia, dove l'Autorità locale per la protezione dei dati ha istituito una *sandbox* dedicata allo sviluppo di soluzioni di intelligenza artificiale responsabile[53]. Questa iniziativa mira a promuovere l'adozione di tecnologie di intelligenza artificiale che rispettino standard etici e siano in linea con i requisiti di protezione dei dati.

Oltre al caso della Norvegia, merita attenzione il progetto pilota di *sandbox* normativa istituito in Spagna[54]. Lanciato nel giugno 2022 in collaborazione con la Commissione europea, il pilot spagnolo mirava a testare sistemi di IA ad alto rischio e a uso generale in vista dell'entrata in vigore dell'AI Act. Questo progetto, aperto anche ad altri Stati membri, rappresenta il primo tentativo di una *sandbox* normativa paneuropea, con l'obiettivo di condividere i risultati con l'intera comunità europea[55].

Da quanto precede, si evince come, in tale contesto, l'AI Act emerga come un caso di studio centrale per questo lavoro, rappresentando un punto di riferimento unico per l'esame delle sfide e delle potenzialità delle *sandboxes* normative[56] nel quadro normativo di diritto dell'Unione europea.

Il considerando 138 sottolinea come l'intelligenza artificiale rappresenti una famiglia di tecnologie in rapida evoluzione, richiedendo sia una supervisione normativa che un ambiente sicuro e controllato per la sperimentazione, al fine di promuovere un'innovazione responsabile attraverso l'integrazione di adeguate tutele e misure di mitigazione dei rischi. In quest'ottica, l'articolo 57 del

Nella fase di transizione verso la regolamentazione ufficiale, il Ministero della Salute di Singapore ha iniziato a pubblicare l'elenco dei fornitori di servizi di telemedicina diretta che hanno dimostrato consapevolezza dei rischi e dei benefici della telemedicina, adottato misure per affrontare questi rischi e accettato di rispettare le linee guida per una pratica sicura stabilite dal Ministero.

51. Ministry of Health of Singapore, *Regulatory sandbox - The Licensing Experimentation and Adaptation Programme (LEAP) by MOH supports innovative healthcare services through regulatory sandboxes*, 2024
52. Sherkow 2022.
53. Datatilsynet, *Regulatory privacy sandbox*.
54. Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.
55. Il pilot si propone di chiarire i requisiti di conformità dell'AI Act, trasferire il know-how alle aziende partecipanti e sviluppare linee guida e standard utili a livello europeo. Le attività pratiche includono workshop, consulenze personalizzate e sessioni formative per supportare le imprese nel testare e adeguare i loro sistemi di IA ai requisiti normativi. Il progetto prevede due gruppi di lavoro: uno operativo, focalizzato sul supporto alle aziende, e uno analitico, incaricato di elaborare la documentazione e le linee guida basate sui risultati del pilot. La durata complessiva del progetto è di tre anni, con scadenza nel 2025. Il successo del pilot dipenderà dalla collaborazione delle aziende partecipanti, che dovranno condurre una valutazione di conformità, garantire il monitoraggio post-sperimentazione e presentare report al comitato di coordinamento.
56. Baldini–Francis 2024; Ranchordas–Vinci 2024; Bagni 2023.

Regolamento stabilisce che gli Stati membri provvedano affinché le autorità competenti istituiscano almeno uno[57] spazio di sperimentazione normativa per l'IA, a livello regionale o locale, oppure in collaborazione con le autorità di altri Stati membri, o anche da parte del Garante europeo della protezione dei dati (par. 3).

Un aspetto fondamentale del regime normativo introdotto dall'AI Act è disciplinato dall'articolo 58, il quale stabilisce i requisiti specifici che devono essere soddisfatti dai partecipanti alle *sandboxes*. In particolare, si prevede che le autorità competenti garantiscano un monitoraggio continuo delle attività svolte negli spazi di sperimentazione, verificando che queste rispettino i principi di sicurezza e trasparenza. Si introduce inoltre l'obbligo per i partecipanti di redigere rapporti periodici che descrivano i progressi compiuti e gli eventuali rischi identificati durante la sperimentazione. Questo obbligo è volto a garantire che i sistemi sviluppati nelle *sandboxes* rispettino i requisiti normativi fin dalle prime fasi di progettazione.

Tali spazi di sperimentazione normativa sono concepiti per fornire "un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi innovativi per un periodo limitato prima della loro immissione sul mercato o della loro messa in servizio" (par. 5) e possono anche includere test condotti in "condizioni reali", pur restando soggetti a controlli nell'ambito della *sandbox*.

La norma prevede, inoltre, il coinvolgimento delle autorità nazionali per la protezione dei dati e di quelle responsabili dell'accesso ai dati nelle attività di queste *sandboxes*, con compiti di supervisione entro i limiti delle loro competenze (par. 10). Restano invariati i poteri di controllo e intervento delle autorità competenti (par. 11), mentre i partecipanti alla *sandbox* sono tenuti a rispondere per eventuali danni causati a terzi durante la sperimentazione, secondo le normative vigenti (par. 12).

Le autorità nazionali competenti devono presentare annualmente una relazione all'Ufficio per l'IA, istituito dalla Commissione ai sensi dell'art. 64, e al Comitato europeo per l'intelligenza artificiale di cui all'art. 65 (composto da rappresentanti di ciascuno Stato membro), e che contiene "informazioni sui progressi e sui risultati dell'attuazione di tali spazi di sperimentazione, comprese le migliori pratiche, gli incidenti, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione ed eventuale revisione del presente regolamento, inclusi i rispettivi atti delegati e di esecuzione, e sull'applicazione di altre disposizioni di diritto dell'Unione soggette a controllo da parte delle autorità competenti nell'ambito dello spazio di sperimentazione". A tal riguardo, si deduce, da una interpretazione letterale della disposizione, che la relazione dell'Autorità di controllo sull'andamento degli spazi di sperimentazione normativa possa svolgere un ruolo propulsivo nella revisione dell'AI Act. A ciò si aggiunge che l'articolo 58, paragrafo 6, consente di raccogliere dati e risultati sperimentali che potranno essere utilizzati dalla Commissione per valutare la necessità di modificare il quadro normativo vigente, promuovendo un costante aggiornamento legislativo in linea con l'evoluzione tecnologica.

Questo implica che tali spazi di sperimentazione normativa non solo, di fatto, operano come ambienti controllati per l'innovazione, ma potrebbero anche contribuire all'evoluzione del quadro normativo dell'Unione, offrendo raccomandazioni e suggerendo adattamenti futuri.

Infine, merita menzione l'articolo 60, che consente la sperimentazione di sistemi di IA ad alto rischio[58] "in condizioni reali al di fuori degli spazi di sperimentazione normativa", ovvero senza i consueti controlli, purché vengano rispettate condizioni e garanzie specifiche. In tali casi, è richiesto il rispetto di un "piano di prova in condizioni reali", definito come "un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali". Sarà compito della Commissione, tramite atti di esecuzione, specificare gli elementi da includere nel piano di prova.

L'articolo 61 stabilisce che, per le sperimentazioni condotte al di fuori delle *sandboxes* normative, i partecipanti devono fornire il loro consenso informato, come indicato nel titolo dell'articolo

57. Sul punto, vale la pena precisare che è stato il Parlamento europeo a porre maggiore enfasi sulla necessità di incentivare le *regulatory sandboxes*. V. Rugani 2024, pp. 8-9.

58. Truby et al. 2022.

stesso, "Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA". Tale disposizione è considerata dal legislatore dell'Unione una garanzia essenziale, poiché le sperimentazioni si svolgono al di fuori del quadro regolamentato delle *sandboxes*[59]. Si rileva, inoltre, che la possibilità di condurre prove in condizioni reali fuori dagli spazi di sperimentazione non era prevista nella proposta iniziale della Commissione, ma è stata introdotta dal Consiglio per incentivare un apprendimento basato su evidenze[60].

Le osservazioni sinora formulate conducono inevitabilmente a un'ulteriore indagine giuridica più approfondita sullo status normativo degli spazi di sperimentazione normativa. In particolare, fino a che punto questi strumenti rappresentano un equilibrio efficace tra promozione dell'innovazione e rispetto delle normative? E quali sono le conseguenze giuridiche del loro utilizzo in contesti regolatori diversificati?

Tali interrogativi, cui si cercherà di rispondere nei paragrafi successivi, non solo aprono nuove prospettive per il diritto, ma suggeriscono anche di considerare le *sandboxes* come strumenti in grado di promuovere l'innovazione. Allo stesso tempo, queste strutture emergono come potenziali catalizzatori di un cambiamento significativo nel modo di concepire la regolamentazione in un contesto caratterizzato da rapide e costanti trasformazioni. Le esperienze nazionali, come quella norvegese e spagnola, sembrano suggerire che il successo delle *sandboxes* dipenderà in larga misura dalla collaborazione tra autorità di regolazione e soggetti privati, nonché dall'adozione di un approccio flessibile ma rigoroso.

Sebbene, come già sostenuto in apertura, l'AI Act sia stato esaminato in questo lavoro come un caso di studio paradigmatico, è opportuno precisare che le osservazioni qui condivise non pretendono di fornire una trattazione esaustiva delle disposizioni contenute nel regolamento. L'AI Act, infatti, costituisce solo uno dei contesti applicativi possibili, scelto per la sua centralità e attualità, ma non esaurisce la varietà di scenari in cui tali strumenti regolatori potrebbero essere sperimentati, come dimostrato dall'analisi dei diversi casi pratici affrontati nel contributo.

3. Sperimentando si impara (…e si innova)?

La regolamentazione delle innovazioni tecnologiche rappresenta una sfida complessa e articolata per due principali motivi.

Innanzitutto, quello di innovazione è un concetto difficile da definire con precisione[61] e tanto più da misurare, il che rende complicato il tentativo di normarlo. Tra le definizioni più autorevoli[62]

59. Buocz–Pfotenhauer–Eisenberger 2023.

60. "With a view to creating a legal framework that is more innovation-friendly and to promoting evidence-based regulatory learning, the provisions concerning measures in support of innovation have been substantially modified compared to the Commission proposal", *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, Press release, 9 December 2023..

61. Garnett–Van Calster–Reins 2018.

62. Il principio dell'innovazione, introdotto nel 2013 dal Forum Europeo del Rischio (ERF), rappresenta un tentativo ambizioso di influenzare l'agenda normativa europea. Nato sotto l'egida di un gruppo di lobby industriali che includeva settori chiave come quelli dei combustibili fossili, dell'industria chimica e, inizialmente, del tabacco, l'ERF ha rapidamente acquisito rilievo grazie al sostegno di grandi aziende e organizzazioni come la BusinessEurope. La sua affermazione è stata strategicamente sostenuta attraverso un'intensa attività di lobbying, culminata nella sua prima comparsa in un documento ufficiale dell'Ue nel 2015. L'ERF ha saputo costruire una rete di alleanze che gli ha permesso di accedere a tavoli decisionali di alto livello. Particolarmente rilevante è stato il ruolo della presidenza olandese nel 2016, che ha organizzato una conferenza internazionale dedicata al tema e promosso l'inserimento del principio dell'innovazione nelle conclusioni del Consiglio Competitività. L'adozione ufficiale da parte del Consiglio ha portato la Commissione europea a creare una Innovation Principle Taskforce, con l'obiettivo di monitorare e integrare questo principio nelle future iniziative legislative e politiche. Parallelamente, la Commissione ha avviato un dibattito accademico attraverso il programma Horizon 2020, sollevando una questione cruciale: come bilanciare il principio dell'innovazione con il principio di precauzione, spesso percepiti come in contrasto. Tuttavia, il principio dell'innovazione non è stato privo di controversie. Nel

a livello internazionale vi è quella proposta dal Manuale di Oslo dell'OCSE che, nella sua versione più recente, descrive l'innovazione come "un prodotto o processo nuovo o migliorato (o una loro combinazione) che si differenzia significativamente dai prodotti o processi precedenti dell'unità e che è stato reso disponibile agli utenti potenziali (prodotto) o introdotto nell'uso da parte dell'unità stessa (processo)"[63].

Questa definizione mette in evidenza tre aspetti fondamentali: l'innovazione può riguardare sia novità assolute che miglioramenti di soluzioni esistenti; si applica tanto a prodotti quanto a processi già in uso; e, per essere considerata tale, deve essere accessibile agli utenti.

In secondo luogo, regolamentare il cambiamento tecnologico è complicato perché i prodotti innovativi possono destabilizzare il sistema normativo esistente, sollevando dubbi sulla sua adeguatezza e legittimità. Tale difficoltà nasce in gran parte dalla già segnalata discrepanza tra il rapido progresso della tecnologia e la lentezza con cui le risposte normative si sviluppano. Tuttavia, le tecnologie in continua evoluzione sfidano i metodi tradizionali di regolamentazione non solo a causa, come sopra rilevato, della lentezza della risposta normativa, ma anche per le asimmetrie informative che si creano tra innovatori e regolatori[64]. In particolare, la mancanza di dialogo tra autorità di regolazione e imprese è considerata una delle cause principali di questa disconnessione tra processo innovativo e regolazione.

In questo contesto, l'adozione di sandboxes normative e di altre politiche finalizzate a favorire l'innovazione riflette una crescente consapevolezza dell'importanza di armonizzare la regolazione delle nuove tecnologie e le innovazioni tecnologiche, oltre che della necessità di incentivare una maggiore collaborazione tra legislatore, parti interessate e innovatori. Questo orientamento trova giustificazione nella convinzione che un approccio regolatorio favorevole all'innovazione possa contribuire significativamente alla competitività e alla capacità innovativa dell'Unione.

Un esempio di tale posizione emerge dalla *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, che auspica "un'azione responsabile e diligente da parte di tutti gli attori, pubblici e privati, nell'ambiente digitale."[65] Altre iniziative, come la *Nuova agenda europea per l'innovazione*[66] e il *Piano industriale del Green Deal per l'era a zero emissioni nette*[67], mettono in luce

2018, quando è stato inserito nel preambolo del regolamento di Horizon Europe, ha suscitato un ampio dibattito politico. Più di un terzo degli eurodeputati ha sostenuto un emendamento per rimuoverne il riferimento, evidenziando le tensioni tra il sostegno all'innovazione e la tutela dei principi precauzionali tradizionali. Si v. Saltelli–Dankel–Di Fiore et al. 2022.

63. Traduzione dell'A.; cfr. OECD 2018.

64. Questo fenomeno è ben illustrato dal cosiddetto dilemma di Collingridge, secondo cui all'emergere di un'innovazione i regolatori esitano a intervenire a causa della scarsa disponibilità di informazioni. Tuttavia, quando finalmente ottengono informazioni sufficienti, potrebbe essere troppo tardi, poiché la tecnologia potrebbe essere cambiata o la regolamentazione potrebbe non essere più in grado di contenere i rischi e gli effetti collaterali. In sintesi, i regolatori possono generalmente influenzare lo sviluppo di una tecnologia solo nelle sue prime fasi. Tuttavia, in questa fase iniziale, non dispongono ancora delle informazioni necessarie per comprendere pienamente l'impatto sociale della nuova tecnologia. Successivamente, quando la tecnologia è ormai radicata nella società e i regolatori hanno raccolto maggiori informazioni sui suoi effetti, potrebbe non essere più possibile influenzarne lo sviluppo: Collingridge 1982. V. anche Genus–Stirling 2018.

65. Capitolo 1, 1(c), Parlamento europeo, Consiglio, Commissione europea, "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" (2023/C 23/01), 26 gennaio 2022.

66. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Una nuova agenda europea per l'innovazione", COM/2022/332, 5 luglio 2022.

67. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Un piano industriale del Green Deal per l'era a zero emissioni nette", COM/2023/62, 1 febbraio 2023.

la complessità della regolamentazione dell'innovazione, criticando una visione dell'innovazione limitata a considerazioni economiche e aziendali, che può risultare insensibile agli impatti su sostenibilità, Stato di diritto e diritti umani.

In linea con queste prospettive, nelle Conclusioni precedentemente menzionate, il Consiglio ha individuato nel principio di innovazione[68] un elemento strategico per la creazione di strumenti normativi più efficienti, coerenti e prevedibili, ma anche capaci di rispondere a esigenze future, promuovendo la sostenibilità e la resilienza.

L'introduzione di tale principio ha incentivato il ricorso agli spazi di sperimentazione normativa, strumenti capaci di favorire un'evoluzione coordinata e proattiva del progresso tecnologico in parallelo all'adattamento normativo. Grazie alla loro natura temporanea, flessibile e adattabile, questi strumenti offrono l'opportunità di guidare lo sviluppo di innovazioni responsabili.

Essendo misure transitorie, le *sandboxes* normative consentono di affrontare sfide emergenti con maggiore flessibilità, riducendo il rischio di un'obsolescenza delle norme e di un disallineamento con la realtà pratica, con possibili ripercussioni per le imprese in termini di costi, incertezza e perdita di competitività.

Inoltre, le *sandboxes* normative permettono alla regolamentazione di adattarsi in modo più rapido ai valori sociali in evoluzione e agli obiettivi strategici di più ampio respiro. Regolare l'innovazione incorporando valori sociali, etici e di sostenibilità richiede ai legislatori di individuare e bilanciare tali valori, prendendo in considerazione un'ampia varietà di interessi nella costruzione del quadro normativo.

Tale approccio implica inevitabilmente una maggiore partecipazione di attori non statali nel processo decisionale. Da un lato, gli innovatori possono avvalersi di un ambiente normativo specificamente progettato per testare l'introduzione delle loro soluzioni sul mercato, sotto la supervisione delle autorità competenti e con una maggiore sicurezza normativa; dall'altro, ai regolatori è data l'opportunità di comprendere meglio le innovazioni emergenti, ridurre le asimmetrie informative tipiche del processo innovativo e stabilire un contesto sperimentale adeguato.

In linea con ciò, l'OCSE ha recentemente sottolineato[69], con riferimento all'intelligenza artificiale, che le *sandboxes* normative possono costituire strumenti efficaci per regolare e gestire tecnologie emergenti, soprattutto se integrate con altri meccanismi di regolazione.

3.1. Quali sfide nell'implementazione delle *regulatory sandboxes*?

All'idea che gli spazi di sperimentazione normativa possano favorire un'innovazione responsabile si contrappongono tuttavia alcune questioni rilevanti che meritano un approfondimento.

In primo luogo, come già evidenziato, nell'ordinamento giuridico europeo non vi è una definizione di *sandboxes* normative univoca né un quadro istituzionale che ne disciplini la creazione. Questa lacuna potrebbe creare incertezze tra i regolatori e portare a una frammentazione del mercato unico europeo, oltre a generare equivoci sulle funzioni specifiche delle sandboxes normative, confondendole con altri strumenti sperimentali. Tuttavia, è proprio grazie alla loro flessibilità che le sandboxes possono offrire un valore aggiunto, permettendo ai regolatori di osservare in tempo reale l'impatto delle tecnologie testate e ai soggetti regolati di operare in un contesto normativo temporaneamente adattato alle loro esigenze.

In risposta a questa esigenza, l'OCSE ha tentato di proporre per la prima volta una classificazione delle *sandboxes* normative e di altri strumenti sperimentali[70], basandosi su criteri condivisibili a livello internazionale. La classificazione proposta considera due dimensioni principali: la sfera di applicazione (privata, pubblica o ibrida) e l'ambito di intervento (specifico per norme, orientato alla tecnologia, generico/intersettoriale o legato a regtech/govtech).

A supporto di questa iniziativa, la Commissione europea, nel luglio 2023, ha pubblicato un

68. V. Simonelli–Renda 2019.

69. OECD 2023.

70. *Ibidem*.

documento di lavoro[71] che fornisce indicazioni per distinguere le *sandboxes* normative da altri strumenti come progetti pilota, laboratori di prova e ambienti di test, evidenziando la necessità di differenziazioni chiare tra i vari approcci.

Un ulteriore aspetto critico da considerare riguarda la compatibilità delle *sandboxes* normative con il principio di uguaglianza[72]. Questi strumenti, spesso progettati per settori specifici o per affrontare sfide regolatorie mirate, sono strutturati in funzione delle esigenze dei partecipanti. Tuttavia, la loro implementazione potrebbe sollevare perplessità in relazione al principio di parità di trattamento, in quanto l'accesso privilegiato alle *sandboxes* può determinare uno squilibrio competitivo. I soggetti ammessi, infatti, beneficiano di deroghe normative che non sono estese agli altri operatori di mercato.

Questa differenziazione di trattamento potrebbe entrare in contrasto con quanto stabilito all'articolo 20 della Carta dei diritti fondamentali dell'Unione europea, in virtù del quale situazioni comparabili non devono essere trattate in modo diverso e situazioni diverse non devono essere trattate allo stesso modo, salvo che tale trattamento sia oggettivamente giustificato[73].

Tale principio risulta particolarmente rilevante nel contesto degli spazi di sperimentazione normativa, come evidenziato dalla giurisprudenza della Corte di giustizia nel caso *Société Arcelor Atlantique*, definito dall'Avvocato Generale Maduro come una questione relativa ai "rapporti, per loro natura dialettici, tra la pratica della sperimentazione legislativa e le esigenze normative della parità di trattamento"[74].

Nel caso di specie, la Corte non si è espressa direttamente sul tema della parità di trattamento in relazione alla legislazione sperimentale, tuttavia, pur riconoscendo le differenze concettuali tra il regime normativo[75] analizzato e il quadro giuridico delineato per gli spazi di sperimentazione normativa, i criteri definiti dall'Avvocato generale Maduro offrono un quadro utile per valutare la loro coerenza con il principio di parità di trattamento.

Innanzitutto, nelle sue Conclusioni, l'Avvocato generale ha chiarito che la discriminazione derivante da norme sperimentali può essere compatibile con il principio di parità di trattamento solo se sono rispettate alcune condizioni fondamentali, segnatamente: (i) le misure sperimentali devono avere carattere transitorio e (ii) il loro ambito deve essere definito da criteri oggettivi, strettamente connessi alla materia e agli obiettivi della normativa in questione.

Applicando questi criteri agli spazi di sperimentazione normativa delineati, ad esempio, nell'AI Act si osserva che, in primo luogo, benché il quadro normativo delle *regulatory sandboxes* sia concepito come permanente, i singoli esperimenti condotti al suo interno sono limitati nel tempo, con una durata proporzionata alla complessità e alla portata del progetto.

In secondo luogo, il regime delle *sandboxes* mira a creare un sistema giuridico che favorisca l'innovazione e risulti resiliente ai cambiamenti, mentre gli scopi delle singole sperimentazioni variano in base alla tipologia di sistema di intelligenza artificiale testato e al suo contesto applicativo.

Inoltre, il regolamento sull'IA prevede che la Commissione europea stabilisca, tramite atti di esecuzione, criteri oggettivi per la selezione dei partecipanti agli spazi di sperimentazione normativa.

Si può dunque inferire che, qualora tali criteri si basino su parametri come il grado di innovatività e la maturità tecnologica, piuttosto che sul settore di appartenenza, i requisiti delineati dall'Avvocato generale nel caso *Arcelor* risulterebbero soddisfatti.

71. Commission Staff Working Document, *Regulatory learning in the EU. Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy*, 25 July 2023, SWD(2023) 277/2.
72. Conclusioni dell'Avvocato generale Maduro, causa C-127/07, *Société Arcelor Atlantique*, par. 46.
73. Corte di giustizia, *Polonia/Consiglio*, causa C-273/04; Corte di giustizia, *Nagy*, causa C-21/10, par. 47; Corte di giustizia, *TP*, causa C-356/12 par. 81; Martin 2019.
74. Conclusioni dell'Avvocato generale Maduro, cit., par. 2.
75. Il caso riguardava una direttiva che istituiva un sistema di scambio di quote di emissione, applicabile al settore siderurgico ma non a quelli dell'alluminio e della plastica.

Occorre infine evidenziare, come sottolineato dall'Avvocato generale Maduro, che la Corte di giustizia riconosce al legislatore un'ampia discrezionalità, in particolare quando le decisioni legislative implicano scelte di carattere politico, economico o sociale, oppure richiedono valutazioni di elevata complessità[76]. In questi casi, il sindacato giurisdizionale della Corte si limita alla "ricerca di un errore manifesto di valutazione nelle scelte operative"[77].

Ancora, la possibilità di istituire *sandboxes* in ciascuno Stato membro ha sollevato dubbi sul potenziale rischio di frammentazione all'interno dell'ordinamento giuridico europeo. A tal riguardo, quantomeno per la disciplina sull'intelligenza artificiale, l'AI Act cerca di rispondere a queste preoccupazioni; infatti, come già detto, l'articolo 58 dispone che la Commissione adotti atti di esecuzione "che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'IA". Inoltre, l'articolo prevede altresì che suddetti atti di esecuzione comprendano principi comuni riguardanti criteri di ammissibilità e selezione per la partecipazione alla sandbox, le procedure per la domanda, partecipazione, monitoraggio e uscita dalla *sandbox*, nonché per la sua cessazione, oltre ai termini e alle condizioni applicabili ai partecipanti.

Ciononostante, permangono molte incertezze sull'uso di questi strumenti, anche nel contesto dell'AI Act. Ad esempio, la portata e la natura delle *sandboxes* normative non sono chiaramente definite nel Regolamento. L'articolo 57 elenca come obiettivi delle *sandboxes* normative per l'IA: migliorare la certezza del diritto al fine di conseguire la conformità normativa, condividere le migliori pratiche, promuovere l'innovazione e la competitività, contribuire all'apprendimento normativo basato su dati concreti e agevolare e accelerare l'accesso al mercato dell'UE per i sistemi di IA.

Tuttavia, potrebbe essere necessaria una maggiore chiarezza riguardo al design e alla classificazione delle sandboxes, poiché alcune potrebbero avere una natura sperimentale mentre altre potrebbero servire principalmente come strumenti di conformità collaborativa. Invero, affinché la fase di sperimentazione possa portare a risultati validi, è necessario che gli obiettivi e le ipotesi da testare siano chiaramente definiti sin dall'inizio dell'esperimento, o addirittura precedentemente. Un esempio concreto di questo meccanismo di mutuo vantaggio può essere individuato nelle *sandboxes* adottate per il settore fintech. In tali contesti, le autorità di vigilanza finanziaria collaborano con start-up e istituti bancari per testare nuovi servizi digitali. Da un lato, i regolatori possono ottenere preziose informazioni sulle potenziali implicazioni normative di nuove tecnologie o di servizi di pagamento innovativi, migliorando così la certezza del diritto e adattando le norme in modo più informato. Dall'altro lato, i soggetti regolati beneficiano di un ambiente normativo più flessibile e meno oneroso durante la fase di sperimentazione, favorendo l'innovazione e l'accesso al mercato.

È essenziale che tutte le parti coinvolte comprendano quali sono gli scopi della *sandbox* normativa, per quale motivo sono state stabilite specifiche condizioni di ingresso e uscita, e se la struttura sperimentale potrebbe essere generalizzata per l'intera società. In virtù della loro natura, le *sandboxes* normative, specie quando introducono deroghe sperimentali, richiedono una chiara identificazione sia delle variabili indipendenti sia di quelle dipendenti.

Come stabilito dall'articolo 60 dell'AI Act, che disciplina il funzionamento di tali strumenti, una *sandbox* normativa può prevedere la sperimentazione di prodotti o servizi in un contesto reale. Tuttavia, in tali circostanze, il controllo sulle variabili estranee risulta intrinsecamente limitato. Di conseguenza, è indispensabile adottare misure che evitino un'interpretazione erronea dei risultati, salvaguardando così l'integrità e l'affidabilità delle sperimentazioni condotte.

A tal fine, nella formulazione e personalizzazione[78] delle ipotesi sperimentali, è opportuno utilizzare una terminologia chiara e accessibile, garantendo che tutti i soggetti interessati abbiano piena consapevolezza degli obiettivi, delle modalità e delle finalità del test. La strutturazione delle ipotesi, inoltre, dovrebbe includere l'individuazione di diverse opzioni per l'implementazione

76. Conclusioni dell'Avvocato generale Maduro, cit., par. 35.

77. *Ibidem*.

78. Cfr. Johnson 2023.

dell'intervento, accompagnata da una raccomandazione motivata sulla soluzione preferibile[79].

In buona sostanza, volendo trarre le fila di quanto sinora detto, l'approccio sperimentale delle *regulatory sandboxes*, sia per l'ambito dell'intelligenza artificiale che per altre soluzioni[80], essendo concepito per testare misure regolatorie in un ambiente controllato, consente di raccogliere dati empirici preziosi per orientare le future decisioni normative in modo più informato e basato sull'evidenza. Tale configurazione richiede, per sua natura, una stretta collaborazione tra il legislatore e gli innovatori, configurandosi dunque come uno strumento di coregolazione[81], meccanismo mediante il quale "un atto legislativo dell'Unione conferisce la realizzazione degli obiettivi definiti dal legislatore ai soggetti interessati riconosciuti in un determinato settore"[82]. Tuttavia, questa interazione solleva al contempo potenziali criticità, tra cui il rischio di un condizionamento (c.d. *regulatory capture*) del potere legislativo da parte delle imprese partecipanti.

Per la rilevanza che questa criticità presenta nel complessivo assetto giuridico dell'Unione, si ritiene necessaria una trattazione a parte.

4. La (necessaria) sinergia tra pubblico e privato negli spazi di sperimentazione normativa

Nell'ordinamento giuridico europeo, il concetto di coregolazione si inserisce in un dibattito complesso che riguarda sia la legittimità sia l'efficacia delle decisioni normative. Questa modalità di governance rappresenta un modello innovativo, nel quale gli attori privati assumono un ruolo diretto nella definizione e nell'attuazione di norme e standard, operando spesso in collaborazione o sotto la supervisione di istituzioni pubbliche. Tuttavia, il termine coregolazione non deve essere interpretato come una semplice delega normativa ai privati, bensì come una "partnership" in cui gli attori pubblici stabiliscono i parametri entro cui i privati operano, assicurando un controllo continuo e l'osservanza degli obiettivi di interesse generale.

Questo approccio alla regolazione si è sviluppato in risposta alla crescente complessità delle società moderne e alla necessità di affrontare questioni tecniche altamente specializzate, che richiedono competenze spesso non presenti nelle istituzioni pubbliche tradizionali. La coregolazione, infatti, non si limita a un rapporto di affiancamento tra la sfera pubblica, rappresentata dal legislatore, e la sfera privata, incarnata dalle imprese, ma comporta una vera e propria integrazione funzionale.

In altre parole, questo meccanismo offre vantaggi significativi, consentendo una maggiore flessibilità e rapidità nel rispondere a problematiche emergenti, specialmente in settori ad alta dinamicità, come la tecnologia, l'ambiente e i servizi finanziari, in quanto il legislatore dell'Unione stabilisce un quadro normativo generale, delegando agli attori privati il compito di dettagliare le modalità

79. Ad esempio, nell'ambito di una *sandbox* normativa, i regolatori potrebbero valutare l'ipotesi che una riduzione degli oneri normativi, come la semplificazione delle licenze di ingresso al mercato, possa incentivare l'innovazione, in particolare da parte delle piccole e medie imprese.

80. Ad esempio, nel settore bancario, finanziario e assicurativo, oltre che nell'ambito di nuove tecnologie come la blockchain. Per il primo settore, v. Banca d'Italia, *Sandbox regolamentare*: "Attraverso lo strumento della sandbox, si persegue l'obiettivo di sostenere la crescita e l'evoluzione del mercato italiano grazie all'introduzione di modelli innovativi nel settore bancario, finanziario e assicurativo garantendo, al contempo, adeguati livelli di tutela dei consumatori e di concorrenza, preservando la stabilità finanziaria. Allo stesso tempo, le autorità responsabili per la regolamentazione potranno osservare le dinamiche dello sviluppo tecnologico e individuare gli interventi normativi più opportuni ed efficaci per agevolare lo sviluppo del FinTech, contenendo già in avvio la diffusione di potenziali nuovi rischi. Tramite la partecipazione alla sandbox, gli operatori possono testare prodotti e servizi innovativi in costante dialogo e confronto con le autorità di vigilanza, anche richiedendo eventuali deroghe normative nella fase di sperimentazione". Per le iniziative in materia di *blockchain* e *distributed ledger technology*, v. European Commission 2023-a.

81. Nell'Accordo Interistituzionale *Legiferare meglio* del 13 aprile 2016 tra Parlamento, Consiglio e Commissione, la coregolazione è denominata "meccanismo di regolamentazione alternativo".

82. Bartoloni 2021.

operative tramite codici di condotta, standard tecnici e altri strumenti autoregolativi.

In quest'ottica, gli spazi di sperimentazione normativa rappresentano strumenti emblematici di coregolazione, poiché consentono agli attori privati di operare in un contesto regolato e monitorato dal legislatore, contribuendo all'evoluzione delle norme attraverso la pratica e la sperimentazione diretta.

Questi strumenti si configurano come ambienti controllati in cui le imprese possono sperimentare nuove soluzioni tecnologiche con una supervisione regolatoria ridotta o adattata, ma sempre nell'ambito di un quadro definito dal legislatore.

In linea generale, la delega di alcune funzioni regolatorie a soggetti privati, anche se limitata e supervisionata, solleva questioni di legittimità rispetto ai valori dell'Unione.

Innanzitutto, la partecipazione di attori privati nella definizione della normativa può generare conflitti di interesse e minare il principio di certezza del diritto, qualora le norme risultino meno chiare e prevedibili rispetto a quelle adottate attraverso il processo legislativo ordinario. Per questo motivo, lo strumento della coregolazione, perchè sia efficace, richiede un solido sistema di supervisione pubblica, capace di garantire che l'interesse generale prevalga su eventuali interessi particolari.

La trasparenza è altresì cruciale per il successo della coregolazione e, quindi, delle *regulatory sandboxes*. In assenza di meccanismi chiari e accessibili per il monitoraggio del processo decisionale, sia in generale sia nello specifico contesto delle *sandboxes*, si rischierebbe di compromettere la fiducia dei cittadini nelle istituzioni europee, fino al punto di alimentare il timore di un'influenza indebita da parte degli attori privati sulle decisioni normative. Questa eventualità è, quantomeno in linea teorica, amplificata dalla natura sperimentale delle *sandboxes*, dove, in assenza di adeguata trasparenza, potrebbe risultare difficile distinguere se le deroghe normative o le linee guida adottate siano giustificate dal progetto sperimentale o se conferiscano indebiti vantaggi competitivi ad alcune imprese, escludendone altre.

Un ulteriore aspetto che merita attenzione riguarda il controllo democratico[83]. In un sistema basato sulla rappresentatività, come quello dell'Unione europea, la delega normativa agli attori privati può minare il principio secondo cui le decisioni che incidono sulla collettività devono essere adottate da soggetti democraticamente legittimati. Tuttavia, si rileva che le forme di coregolazione fondate su un dialogo aperto e continuo con gli stakeholder risultano coerenti con i principi sanciti dai Trattati. L'articolo 10 TUE, infatti, garantisce a ogni cittadino il diritto di partecipare alla vita democratica dell'Unione, valorizzando la necessità che le decisioni siano adottate in modo trasparente e con un approccio il più possibile orientato alla partecipazione diretta dei cittadini. In modo complementare, l'articolo 11 TUE rafforza questa visione richiedendo un dialogo regolare, aperto e inclusivo con le parti interessate, insieme a consultazioni estese e rappresentative.

In questo contesto, le *regulatory sandboxes* rappresentano un'opportunità per concretizzare un modello di governance europea in cui il dialogo tra pubblico e privato diviene un pilastro della legittimità democratica e della costruzione di un quadro normativo condiviso e trasparente. Nel caso delle *regulatory sandboxes* per l'intelligenza artificiale, introdotte dal quadro normativo delineato nell'AI Act, il legislatore ha previsto specifiche misure di mitigazione dei rischi. Tra queste, il coordinamento dei rappresentanti degli Stati membri attraverso il Comitato europeo per l'IA e il rafforzamento dei requisiti di trasparenza, come la pubblicazione di rapporti di valutazione e la giustificazione delle misure adottate. Questi meccanismi mirano a bilanciare l'esigenza di innovazione con la tutela dell'interesse pubblico e la prevenzione di potenziali abusi. Ad ogni modo, le disposizioni previste nel testo normativo potranno essere ulteriormente integrate e rafforzate dagli atti di esecuzione che la Commissione sarà chiamata ad adottare ai sensi dell'articolo 58 del Regolamento.

83. Il principio democratico-rappresentativo nell'ordinamento giuridico europeo si sviluppa su due livelli distinti: da un lato, quello garantito dal Parlamento europeo, il quale rappresenta direttamente i cittadini dell'Unione; dall'altro, quello incarnato dal Consiglio europeo e dal Consiglio, dove gli Stati membri sono rappresentati "dai rispettivi governi, a loro volta democraticamente responsabili dinanzi ai loro parlamenti nazionali o dinanzi ai loro cittadini" (art. 10, par. 2, TUE).

Secondo le linee tracciate, potrebbe risultare utile prevedere l'introduzione di una normativa quadro che definisca principi fondamentali e garanzie minime per lo svolgimento delle sperimentazioni, in contesti diversi da quello dell'intelligenza artificiale. Tale normativa dovrebbe non solo assicurare la tutela degli interessi pubblici, ma anche prevenire possibili distorsioni della concorrenza tra gli operatori economici coinvolti, promuovendo così condizioni di parità e una competizione leale. Questo approccio potrebbe inoltre rafforzare la fiducia nel processo regolatorio, soprattutto nei casi in cui gli spazi di sperimentazione normativa conducano a una modifica della normativa esistente o alla predisposizione di nuove disposizioni, oltre a favorire un'adozione più ampia e consapevole di tali strumenti sperimentali.

5. Osservazioni conclusive

Questo contributo ha analizzato l'evoluzione dell'approccio regolatorio dell'Unione di fronte alle problematiche derivanti dall'emergere di nuove tecnologie, mettendo in evidenza le questioni poste dalla transizione da un modello tradizionale, basato sulla neutralità tecnologica, a uno strumento normativo più dinamico e flessibile.

Questo cambiamento riflette una tensione intrinseca tra la necessità di promuovere l'innovazione tecnologica e quella di garantire la tutela dei diritti fondamentali e degli interessi collettivi, imponendo al legislatore di adottare soluzioni che bilancino entrambi gli obiettivi.

Attraverso l'analisi delle prassi applicative e del recente Regolamento sull'intelligenza artificiale come caso di studio, si è messo in luce il ruolo centrale degli spazi di sperimentazione normativa nel favorire un approccio legislativo più adattabile e basato su evidenze tecniche specifiche. Questi strumenti non solo rappresentano un mezzo per verificare l'efficacia delle disposizioni normative in contesti reali, ma promuovono anche un dialogo costruttivo tra regolatori e innovatori, in linea con i principi democratici e partecipativi sanciti dai Trattati.

Tuttavia, l'introduzione degli spazi di sperimentazione normativa non è priva di potenziali criticità. L'analisi ha evidenziato come tali strumenti pongano interrogativi rilevanti in merito alla trasparenza e all'equità di trattamento, sottolineando la necessità di definire criteri chiari e condivisi per la loro implementazione. Questi ambienti regolatori permettono di sperimentare soluzioni innovative e, in taluni casi, consentono anche di introdurre deroghe mirate alla normativa vigente per testarne la validità e individuare eventuali modifiche necessarie.

L'esempio delle *sandboxes* per l'intelligenza artificiale, introdotte dall'AI Act, sottolinea sia le potenzialità di questi strumenti nel promuovere un'armonizzazione normativa tra gli Stati membri, sia le questioni legate al rischio di frammentazione normativa e di una possibile "cattura regolatoria" da parte degli operatori privati. In questo contesto, ove vengano concesse deroghe normative, è fondamentale garantire un equilibrio tra flessibilità e certezza del diritto, evitando che l'eccezionalità del regime proprio delle *sandboxes* comprometta la coerenza del quadro normativo generale e crei squilibri nelle condizioni del mercato in virtù del potenziale vantaggio competitivo che le imprese partecipanti alla sperimentazione potrebbero acquisire.

Nel complesso, gli spazi di sperimentazione normativa si configurano come un'opportunità per ripensare il rapporto tra regolazione e innovazione, aprendo la strada a un modello di governance più reattivo e basato su evidenze empiriche. Tuttavia, la loro reale efficacia dipenderà dalla capacità del legislatore non solo di adottare un approccio equilibrato, ma anche di strutturare un sistema di supervisione che garantisca inclusività, trasparenza e accountability. Nel caso del Regolamento sull'intelligenza artificiale, molto dipenderà dagli atti di esecuzione della Commissione europea. Mentre, negli altri settori, sarebbe auspicabile l'introduzione di un quadro normativo uniforme, capace di affrontare le problematiche evidenziate e promuovere soluzioni coerenti con i valori dell'Unione.

In definitiva, se implementate secondo criteri oggettivi e adeguati, le *sandboxes* normative potrebbero, non solo contribuire alla definizione di un quadro normativo più resiliente e adeguato alle sfide del futuro, ma anche rafforzare alcuni valori fondamentali dell'Unione europea: trasparenza, inclusione e sostenibilità.

La citazione posta in apertura di questo contributo – "[c]ostruire teorie prima di aver raccolto i fatti è un errore madornale: conduce ad adattare i fatti alle teorie, invece che adattare le teorie ai fatti"

– rappresenta una sintesi efficace del principio teorico e funzionale che anima gli spazi di sperimentazione normativa. Questi strumenti, attraverso un approccio fondato su evidenze empiriche, permettono di adattare le normative alle esigenze pratiche, evitando così l'errore di costruire regole astratte, disconnesse dalla realtà e, perciò, difficilmente applicabili.

Riferimenti bibliografici

H. Allen (2020), *Sandbox Boundaries*, in "Vanderbilt Journal of Entertainment & Technology Law", vol. 22, 2020, n. 2

H. Allen (2019), *Regulatory Sandboxes*, in "George Washington Law Review", vol. 87, 2019, n. 3

J. Armour, M. Sako (2020), *AI-enabled business models in legal services: from traditional law firms to next-generation law companies?*, in "Journal of Professions and Organization", vol. 7, 2020, n. 1

A. Attrey, M. Lesher, C. Lomax (2020), *The role of sandboxes in promoting flexibility and innovation in the digital age*, in "OECD Going Digital Toolkit Policy Notes", OECD Publishing, 2020

F. Bagni (2023), *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in "Rivista italiana di informatica e diritto", 2023, n. 2

D. Baldini, K. Francis (2024), *AI Regulatory Sandboxes between the AI Act and the GDPR: The role of Data Protection as a Corporate Social Responsibility*, in "CEUR Workshop Proceedings", vol. 3731, 2024

I. Bar-Siman-Tov (2018), *Temporary legislation, better regulation, and experimentalist governance: An empirical study*, in "Regulation & Governance", vol. 12, 2018, n. 2

M.E. Bartoloni (2021), *La regolazione privata nel sistema costituzionale dell'Unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione*, in "Osservatorio sulle fonti", 2021, n. 3

G. Buchholtz (2020), *Artificial Intelligence and Legal Tech: Challenges to the Rule of Law*, in T. Wischmeyer, T. Rademacher (eds.), "Regulating Artificial Intelligence", Springer, 2020

T. Buocz, S. Pfotenhauer, I. Eisenberger (2023), *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, in "Law, Innovation and Technology", vol. 15, 2023, n. 2

S. Chesterman (2021), *Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity*, in "The American Journal of Comparative Law", vol. 69, 2021, n. 2

D. Collingridge (1982), *Social Control of Technology*, Continuum International Publishing Group Ltd., 1982

Consiglio dell'Unione europea (2020), *Conclusioni del Consiglio sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale*, 16 novembre 2020

A. de Boer (2018), *Scientific assessments in European food law: Making it future-proof*, in "Regulatory Toxicology and Pharmacology", vol. 108, 2018

European Commission (2023), *Better Regulation Toolbox*, 2023

European Commission (2023-a), *Launch of the European Blockchain Regulatory Sandbox* , 2023

European Law Institute (2022), *Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, Report of the European Law Institute, 2022

Expert Group on Regulatory Obstacles to Financial Innovation (2019), *30 Recommendations on regulation, innovation and finance*, 2019

C. Faralli (2019), *Diritti e nuove tecnologie*, in "Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica", 2019, n. 2

Financial Conduct Authority (2017), *Regulatory sandbox lessons learned report*, October 2017

Financial Conduct Authority (2015), *Regulatory sandbox*, November 2015

Financial Stability Board 2020, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications*, 9 October 2020

T. Freund (2003), *Kommunale Standardöffnungs- und Experimentierklauseln im Lichte der Verfassung*, WVB, 2003

S. Garben (2020), *A taste of its own medicine: Assessing the impact of the EU Better Regulation Agenda*, in "European Law Journal", vol. 26, 2020, n. 1-2

K. Garnett, G. Van Calster, L. Reins (2018), *Towards an innovation principle: An industry trump or shortening the odds on environmental protection?*, in "Law Innovation and Technology", vol. 10, 2018, n. 1

A. Genus, A. Stirling (2018), *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, in "Research Policy", vol. 47, 2018, n. 1

M. Gomez Santos (2021), *Régimen jurídico del "regulatory sandbox" en España*, in "Revista de Derecho del Sistema Financiero: Mercados, operadores y contratos", 2021, n. 1

S. Greenstein (2022), *Preserving the rule of law in the era of artificial intelligence (AI)*, in "Artificial Intelligence and Law", vol. 30, 2022, n. 3

M. Hildebrandt, L. Tielemans (2019), *Data protection by design and technology neutral law*, in "Computer Law & Security Review", vol. 29, 2019, n. 5

H.D. Horn (1989), *Experimentelle Gesetzgebung unter dem Grundgesetz*, Duncker & Humblot, 1989

W.G. Johnson (2023), *Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies*, in "Regulation & Governance", vol. 17, 2023, n. 3

B.R. Knight, T.E. Mitchell (2020), *The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege*, in "South Carolina Law Review", vol. 72, 2020, n. 2

E. Leckenby, D. Dawoud, J. Bouvy, P. Jónsson (2021), *The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review*, in "Applied Health Economics and Health Policy", vol. 19, 2021

V. Maaß (2021), *Experimentierklauseln für die Verwaltung und ihre verfassungsrechtlichen Grenzen*, Duncker & Humblot, 2021

D. Martin (2019), *Article 20 CFR*, in M. Kellerbauer, M. Klamert, J. Tomkin (eds.), "The EU Treaties and the Charter of Fundamental Rights: A Commentary", Oxford University Press, 2019

M. Milanesi (2023), *Lo sviluppo delle sandbox regolatorie italiane tra dubbi e opportunità*, in "federalismi.it", 2023, n. 15

OECD (2023), *Regulatory sandboxes in artificial intelligence*, OECD Digital Economy Papers No. 356, OECD Publishing, 2023

OECD (2018), *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation*, 4th Edition, OECD Publishing, 2018

D. Quan (2019), *A few thoughts on regulatory sandboxes*, Stanford University, Stanford PACS, 2019

S. Ranchordás (2020), *Innovation-Friendly Regulation: The Sunset of Regulatory Sandboxes?*, in "Law & Policy", vol. 42, 2020, n. 3

S. Ranchordás, M. van't Schip (2020), *Future-Proofing Legislation for the Digital Age*, in S. Ranchordás, Y. Roznai (edited by), "Time, Law, and Change: An Interdisciplinary Study", Hart Publishing, 2020

S. Ranchordás, V. Vinci (2024), *Regulatory sandboxes and innovation-friendly regulation: between collaboration and capture*, in "Italian Journal of Public Law", vol. 16, 2024, n. 1

G. Rugani (2024), *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle* regulatory sandboxes, in "Quaderni AISDUE", 2024, fasc. speciale n. 2

A. Saltelli, D.J. Dankel, M. Di Fiore et al. (2022), *Science, the endless frontier of regulatory capture*, in "Futures", vol. 135, 2022

J.S. Sherkow (2022), *Regulatory Sandboxes and the Public Health*, in "University of Illinois Law Review", 2022, n. 1

F. Simonelli, A. Renda (2019), *Study supporting the interim evaluation of the innovation principle – Final report*, Publications Office, 2019

J.-H. Stahl (2010), *L'expérimentation en droit français: une curiosité en mal d'acclimatation*, in "Revue Juridique de l'Économie Publique", 2010

H. Surden, M.A. Williams (2016), *Technological Opacity, Predictability, and Self-Driving Cars*, in "Cardozo Law Review", vol. 38, 2016

M. Trapani (2022), L*'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento*, in "Osservatorio sulle fonti", 2022, n. 3

J. Truby, R.D. Brown, I.A. Ibrahim, O. Caudevilla Parellada (2022), *A sandbox approach to regulating high-risk artificial intelligence applications*, in "European Journal of Risk Regulation", vol. 13, 2022

G. Umbach (2024), *Futures in EU governance: Anticipatory governance, strategic foresight and EU Better Regulation*, in "European Law Journal", vol. 30, 2024, n. 3

V. Vaassen (2022), *AI, Opacity, and Personal Autonomy*, in "Philosophy & Technology", vol. 35, 2022

K. Yeung (2017), *Are human biomedical interventions legitimate regulatory policy instruments?*, in R. Brownsword, E. Scotford, K. Yeung (eds.), "The Oxford handbook of law, regulation and technology", Oxford University Press, 2017

V.K. Yordanova (2019), *The Shifting Sands of Regulatory Sandboxes for AI*, in "Centre for IT and IP law blog", July 2019

World Bank Group (2020), *Global Experiences from Regulatory Experiences. Finance, Competitiveness & Innovation Global Practice*, Fintech Note, no. 8, 2020

D.A. Zetzsche, R.P. Buckley, J.N. Barberis, D.W. Arner (2017), *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in "Fordham Journal of Corporate & Financial Law", vol. 23, 2017, n. 1

F. Zunzunegui (2020), *Aproximación al espacio controlado de pruebas, (Commentary on Spanish Regulatory Sandbox Act)*, in "Revista General de Derecho de los Sectores Regulados", Working Paper 6/2020

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0210 • articolo sottoposto a peer review • pubblicato in anteprima il 26 feb. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Arcangelo Leone De Castris

Possibili funzioni di un istituto internazionale per la sicurezza dell'intelligenza artificiale. Un'analisi istituzionale dell'AIEA e dell'IPCC nel contesto delle recenti tendenze sulla governance dell'intelligenza artificiale

I principali attori coinvolti nella governance dell'intelligenza artificiale (IA) in tutto il mondo concordano sul fatto che se da un lato questa tecnologia promette di produrre enormi benefici di natura economica e sociale, dall'altro è necessario implementare dei processi che ne regolino lo sviluppo e l'utilizzo in modo da mitigare i rischi che essa comporta. Diverse istituzioni internazionali – tra cui l'OCSE, il G7, il G20, l'UNESCO e il Consiglio d'Europa – hanno iniziato a sviluppare quadri di governance per lo sviluppo etico e responsabile dell'IA. Nonostante importanti sviluppi in questo senso, ad oggi non esistono dei processi istituzionalizzati al livello internazionale per identificare, misurare e controllare le capacità potenzialmente dannose dell'IA. Con l'obiettivo di contribuire al dibattito accademico sul tema, questo articolo riflette sull'opportunità di creare un istituto internazionale per la sicurezza dell'IA. Partendo dall'analisi delle istituzioni internazionali che si occupano di sicurezza in aree politiche adiacenti all'IA, nonché degli istituti nazionali per la sicurezza dell'IA recentemente costituiti dal Regno Unito e dagli Stati Uniti, l'articolo propone un elenco di funzioni che potrebbero essere svolte da un istituto internazionale per la sicurezza dell'IA. In particolare, l'articolo suggerisce che le possibili funzioni di tale istituto possono essere articolate all'interno di tre categorie: (a) ricerca e cooperazione, (b) audit e verifiche di conformità dei modelli di IA e (c) supporto alla definizione di quadri di governance dell'IA.

Intelligenza artificiale – Governance dell'IA – Sicurezza dell'IA – Etica dell'IA

Possible functions of an international institute for AI safety. An institutional analysis of the IAEA and IPCC in the context of recent trends in AI governance

Most actors involved in governing AI technologies around the world agree that, while AI promises to deliver tremendous benefits to society, appropriate guardrails are required to mitigate its risks. International institutions – including the OECD, the G7, the G20, UNESCO, and the Council of Europe – have started developing frameworks for ethical and responsible AI governance. However, these initiatives alone fall short of addressing the need for institutionalised international processes to identify and assess potentially harmful AI capabilities. This paper contributes to the ongoing conversation on how to address this gap by reflecting on the opportunity to establish an international institution for AI safety. Based on the analysis of international institutions established to address safety considerations in adjacent policy areas and of the newly established national AI safety institutes in the UK and US, this paper identifies a list of functions that could be performed by an international institution for AI safety in three broad areas: (a) technical research and cooperation, (b) safeguards and evaluations, and (c) policymaking and governance support.

Artificial intelligence – AI governance – AI safety – AI ethics

L'Autore è ricercatore associato presso The Alan Turing Institute, Londra

Sommario: 1. Introduzione. – 2. La sicurezza dell'IA nel contesto dell'etica e della governance. – 3. Governance nucleare globale: l'Agenzia Internazionale per l'Energia Atomica. – 4. Governance ambientale: il Panel intergovernativo sul cambiamento climatico. – 5. Rilevanza dei modelli IAEA e IPCC per un istituto internazionale per la sicurezza dell'IA. – 6. Primi passi verso l'istituzionalizzazione di funzioni di governance per la sicurezza dell'IA. – 7. Potenziali funzioni di un istituto internazionale per la sicurezza dell'IA. – 7.1. Ricerca e cooperazione. – 7.2. Audit e verifiche di conformità dei modelli di IA. – 7.3. Supporto tecnico per la definizione di quadri di governance dell'IA. – 8. Conclusione.

1. Introduzione

In risposta alla rapida commercializzazione dei sistemi di intelligenza artificiale (IA) generativa, nel 2023 sono stati lanciati numerosi appelli per una regolamentazione globale dell'IA da parte di figure di spicco in ambito economico e politico[1]. Uno dei temi più dibattuti riguarda la creazione di istituzioni per la governance dell'IA[2]. In particolare, nel periodo precedente al Summit sulla sicurezza dell'IA ospitato dal Regno Unito nel novembre 2023, si è discusso in modo approfondito su quale sia il modello di governance più adeguato, e diversi analisti hanno proposto di prendere spunto dal modello della governance ambientale, con l'*International Panel on Climate Change* (IPCC), e dell'energia atomica, con l'*Agenzia internazionale per l'energia atomica* (AIEA). Tuttavia, tracciare paralleli tra ambiti tematici così diversi presenta il rischio di giungere a conclusioni non del tutto accurate. Inoltre un istituto per la sicurezza dell'IA modellato sugli esempi dell'IPCC o dell'AIEA rischierebbe di ereditare gli stessi problemi che hanno limitato l'efficacia di tali istituzioni[3]. In ogni caso, anche se questi esempi non sono direttamente applicabili alla governance dell'IA, analizzare le misure di governance in ambiti politici adiacenti a quello dell'IA potrebbe comunque fornire lezioni preziose per questo nuovo campo[4].

Partendo da tale ipotesi, questo articolo propone un'analisi di tipo istituzionale dell'AIEA e dell'IPCC[5], analizzandone le funzioni esercitate e i risultati raggiunti e riflettendo sulla loro rilevanza per la governance dell'IA. L'articolo propone inoltre una breve analisi degli istituti nazionali per la sicurezza dell'IA recentemente costituiti nel Regno Unito e negli Stati Uniti. Infine, contestualizzando l'analisi di questi casi di studio all'interno degli attuali sviluppi nell'ambito della governance dell'IA, l'articolo offre un'interpretazione delle funzioni che un ipotetico istituto internazionale per la sicurezza dell'IA potrebbe svolgere. Lo spazio limitato di questa analisi impedisce di offrire un confronto più ampio con altre istituzioni internazionali – ad esempio, l'*International Financial Stability Board* – e con istituti nazionali per la sicurezza dell'IA di più recente creazione – ad esempio,

1. Altman–Brockman–Sutskever 2023; Suleyman–Schmidt 2023; Milmo 2023; Prime Minister's Office 2023; Guterres 2023.
2. Ho–Barnhart–Trager et al. 2023; Marcus–Reuel 2023; Roberts–Hine–Taddeo et al. 2023; Veale–Matus–Gorwa 2023.
3. Afina–Lewis 2023; Stewart 2023; De Pryck–Hulme 2022.
4. Milmo 2023.
5. Steinmo–Thelene–Longstreth 1992.

gli istituti creati in Canada, Singapore, Giappone e Corea del Sud. Questi rimangono importanti casi di studio da approfondire con ricerche future.

Il secondo paragrafo di questo articolo illustra la relazione tra il tema della sicurezza dell'IA e i concetti di etica e governance[6], collocando la creazione di istituzioni per la sicurezza dell'IA nel più ampio panorama globale della governance di questa tecnologia. Il terzo e quarto paragrafo, rispettivamente, offrono un'analisi dei casi di studio dell'AIEA e dell'IPCC, concentrandosi sui loro successi e fallimenti negli ambiti della governance ambientale e nucleare. Il quinto paragrafo riflette sulla rilevanza di entrambi questi modelli per il dibattito in corso sulla governance dell'IA e, in particolare, sulla potenziale creazione di un istituto internazionale per la sicurezza dell'IA. Il successivo paragrafo analizza le recenti iniziative del Regno Unito e degli Stati Uniti relative alla creazione di istituti nazionali per la sicurezza dell'IA, valutandone il mandato istituzionale e confrontandoli con le conclusioni tratte dai casi di studio dell'IPCC e dell'IEAE. Nell'ultimo paragrafo vengono infine elencate le potenziali funzioni di un istituto internazionale per la sicurezza dell'IA sulla base dell'analisi precedentemente svolta.

2. La sicurezza dell'IA nel contesto dell'etica e della governance

Il tema della sicurezza dell'IA è strettamente legato ai due concetti più ampi di etica e governance. Il concetto di etica dell'IA si riferisce all'insieme di valori, principi e tecniche che impiegano standard ampiamente accettati di ciò che è giusto e sbagliato nel guidare lo sviluppo e l'uso delle tecnologie di IA[7]. Nell'ambito dell'etica dell'IA, il termine "sicurezza" viene utilizzato per indicare uno dei principi guida per lo sviluppo di un'IA etica. Sulla base di questo principio, l'IA deve funzionare in modo robusto e sicuro e i rischi che pone devono essere identificati, valutati e gestiti in modo continuativo durante il ciclo di vita delle sue applicazioni. I principi etici possono essere integrati all'interno di processi organizzativi tramite diversi strumenti di governance. Per governance si intende il sistema di organi, regole, pratiche e processi che possono essere impiegati per garantire che l'uso delle tecnologie di IA da parte di un'organizzazione sia compatibile con gli obbiettivi strategici, i requisiti legali e i principi etici dell'organizzazione stessa[8].

Ai fini di questo articolo, il concetto di sicurezza dell'IA si riferisce alla combinazione di due condizioni, una negativa e una positiva: (a) l'assenza di rischi inaccettabili causati dall'uso dell'IA, e (b) l'esistenza di misure di sicurezza per gestire i rischi e i potenziali danni legati all'uso dell'IA[9]. In questo senso, il ruolo di un istituto per la sicurezza dell'IA sarebbe quello di sviluppare e mettere in atto tali misure con lo scopo di prevenire o controllare i rischi posti dalle applicazioni dell'IA.

Il tema della sicurezza dell'IA si inserisce in un complesso contesto di governance internazionale composto da molteplici strumenti di regolamentazione, inclusi trattati e convezioni, principi, accordi quadro, standard tecnici, sviluppati da organismi come ISO e IEC, e sistemi regolatori paralleli, come ad esempio la governance delle piattaforme digitali, la protezione dei dati e della privacy e gli accordi commerciali internazionali. Tra le iniziative di governance internazionale dell'IA di maggior rilievo vi sono i Principi sull'IA dell'OCSE (2019), la Raccomandazione sull'etica dell'IA dell'UNESCO (2022), il Report della Partnership globale sull'IA (2023), il Rapporto sulla Governance dell'IA per l'Umanità dell'ONU (2023), il Processo di Hiroshima del G7 (2023) e la Convenzione sull'IA e i diritti umani del Consiglio d'Europa (2024). Altrettanto importanti iniziative, alcune delle quali con effetti extraterritoriali, esistono anche su scala regionale e nazionale. Ad esempio, il Regolamento europeo sull'IA (EU AI Act) è applicabile a persone fisiche e giuridiche che sviluppano o implementano sistemi di IA che producono effetti all'interno dell'Unione, a prescindere dalla loro residenza legale. Negli Stati Uniti, sebbene non sia prevista l'adozione di leggi sull'IA a livello federale, diversi Stati hanno adottato o stanno considerando regolamenti sul tema. Ad esempio, il Colorado ha approvato il

6. Jobin–Ienca–Vayena 2019.
7. Leslie 2019.
8. Mäntymäki–Minkkinen–Birkstedt–Viljanen 2022.
9. Habli 2023.

disegno di legge SB24-205[10], che fornisce protezione ai consumatori che interagiscono con i sistemi di IA, e il New Jersey ha approvato il disegno di legge S1588, che impone procedure di audit e requisiti di imparzialità a coloro che usano sistemi di IA all'interno di procedure per l'assunzione di personale. Inoltre, il *Risk Management Framework* per l'IA sviluppato dal *National Institute for Standards and Technology* degli Stati Uniti è destinato a svolgere un ruolo importante su scala internazionale come strumento di *soft law*. Simili iniziative sono state adottate anche in diversi altri paesi[11]. In parallelo, organizzazioni internazionali come ISO, IEC e IEEE stanno sviluppando standard tecnici che possono essere adottati volontariamente da aziende e altre organizzazioni per implementare alcuni dei principi etici stabiliti dalle iniziative menzionate in precedenza. Infine, la governance dell'IA si basa anche su una serie di strumenti di governance complementari, tra cui la regolamentazione della protezione dei dati e della privacy[12], la regolamentazione delle piattaforme digitali[13], la regolamentazione del mercato e della concorrenza[14] e la protezione dei diritti umani[15].

All'interno di questo complesso panorama, tuttavia, non esistono funzioni istituzionalizzate per valutare in modo indipendente i rischi e gli sviluppi futuri dell'IA al livello internazionale[16]. Con l'obiettivo di contribuire al dibattito su come colmare questa lacuna, qui di seguito viene proposta una riflessione su come le esperienze dell'AIEA e dell'IPCC possono fornire degli spunti utili a sviluppare nuove soluzioni per la governance internazionale dell'IA.

3. Governance nucleare globale: l'Agenzia Internazionale per l'Energia Atomica

Creata nel 1957 per coordinare la proliferazione nucleare post-bellica su scala globale, l'AIEA è un forum intergovernativo che rappresenta 178 paesi e funge da punto focale globale per la cooperazione scientifica e tecnica nel campo dell'energia nucleare. L'ambito di competenza dell'AIEA include tre aree principali: a) sicurezza, b) ricerca scientifica, c) salvaguardia e controllo. L'obiettivo statutario dell'AIEA comprende funzioni sia "promozionali" sia "regolatorie" in merito all'uso e alla non proliferazione dell'energia nucleare[17]. La funzione promozionale dell'AIEA consiste nell'incoraggiare e assistere la ricerca, lo sviluppo, il finanziamento e la pianificazione di progetti nucleari; sostenere l'applicazione pratica dell'energia atomica per uso pacifico; e, ove necessario, agire come intermediario nei contratti di fornitura di attrezzature e materiali nucleari. Dal punto di vista regolatorio, l'AIEA stabilisce e implementa misure di sicurezza come ispezioni, esami e mandati di approvazione per garantire che materiali fissionabili, attrezzature, strutture e informazioni potenzialmente rischiose non siano utilizzati per scopi militari. L'Agenzia stabilisce inoltre determinati standard di sicurezza e provvede alla loro applicazione pratica.

Una critica frequente all'AIEA riguarda l'apparente contraddizione tra le sua funzioni regolamentari e quelle promozionali[18]. Da un lato, infatti, l'AIEA facilita la condivisione di materiali nucleari, tecnologie e competenze tecniche; dall'altro, tenta di scoraggiare la proliferazione di armi nucleari. Tali osservazioni sono state anche supportate da analisi empiriche secondo cui gli Stati che ricevono assistenza tecnica relativa al ciclo del combustibile nucleare attraverso l'AIEA sono più propensi a creare armi nucleari[19]. Altri studiosi, invece, sostengono il contrario, promuovendo la nozione di "disarmo positivo" ed enfatizzando la funzione inibitoria della cooperazione tecnica nel campo nucleare rispetto allo sviluppo di programmi

10. *Consumer Protections for Artificial Intelligence*, SB24-205 (Col., 2024).
11. Roberts–Ziosi–Osborne 2023.
12. ICO 2023.
13. Veale–Matus–Gorwa 2023.
14. CMA 2024.
15. Leslie–Burr–Aitken et al. 2021.
16. UN AI Advisory Body 2023.
17. Fischer 1997.
18. *Ibidem*; Roehrlich 2022.
19. Brown–Kaplow 2014.

nucleari indipendenti[20]. In effetti, il "paradosso" della regolamentazione nucleare si basa sulla falsa dicotomia tra promozione e regolamentazione e su una concezione parzialmente errata dell'impatto dei programmi di assistenza dell'AIEA. L'impatto di questi programmi sulla proliferazione del nucleare a fini militari, infatti, non è comparabile a quello avuto dagli investimenti delle principali nazioni industrializzate[21].

Un'ulteriore critica mossa all'AIEA riguarda la mancanza di sufficienti poteri esecutivi delle misure e degli standard di sicurezza che essa stabilisce. Ad esempio, l'AIEA ha perso il suo potere di ispezione in Corea del Nord quando il paese ha espulso gli ispettori dell'Agenzia dopo aver receduto dal Trattato di non proliferazione nucleare nel 2023[22]. L'AIEA è stata altrettanto inefficace relativamente allo sviluppo di armi nucleari in Iran, Pakistan e Israele, i quali, non avendo firmato il Trattato di non proliferazione nucleare, non sono formalmente soggetti all'autorità dell'Agenzia[23]. Infine, l'AIEA è stata criticata anche per essere stata sfruttata come strumento di legittimazione delle attività militari di determinati Stati. Secondo questa linea di pensiero, gli Stati Uniti e gli altri membri permanenti del Consiglio di Sicurezza delle Nazioni Unite hanno beneficiato dell'AIEA non solo come iniziativa di pace, ma anche come modo per rafforzare la loro egemonia nucleare[24].

4. Governance ambientale: il Panel intergovernativo sul cambiamento climatico

Istituito nel 1998 dal Programma delle Nazioni Unite per l'Ambiente (UNEP) e dall'Organizzazione Meteorologica Mondiale (WMO), l'IPCC è un'istituzione intergovernativa che riunisce 195 Stati membri e diverse organizzazioni osservatrici. La funzione primaria dell'IPCC è fornire analisi regolari e indipendenti sullo stato della scienza del cambiamento climatico agli Stati membri. Sebbene queste analisi siano rilevanti per lo sviluppo di politiche di governance ambientale, esse non sono in alcun modo vincolanti per gli Stati che le ricevono[25].

L'organo principale dell'IPCC è l'assemblea plenaria, dove i rappresentanti degli Stati membri si incontrano per prendere decisioni di natura strategica. Ad esempio, la plenaria definisce il programma annuale di lavoro del Panel, la struttura e gli obbiettivi principali dei vari gruppi di lavoro e i temi da trattare nel rapporto di valutazione annuale. La plenaria approva il rapporto di valutazione annuale e nomina il *Bureau* dell'IPCC, organo di guida tecnica e strategica del Panel. Infine, la plenaria approva la nomina degli esperti proposti dai governi per redigere i rapporti di valutazione. Gran parte dell'attività dell'IPCC si svolge all'interno dei suoi tre gruppi di lavoro e della *Task Force on National Greenhouse Gas Inventories*. Il primo gruppo di lavoro si occupa della valutazione dello stato della ricerca scientifica sul cambiamento climatico; il secondo studia l'impatto del cambiamento climatico sull'ambiente e sulla società; e il terzo considera potenziali strategie per mitigare i rischi del cambiamento climatico. La *Task Force*, invece, sviluppa metodologie per la misurazione delle emissioni di gas serra.

L'IPCC è stato criticato a causa delle pressioni politiche che possono derivare dal coinvolgimento dei governi nella revisione del lavoro degli scienziati[26]. Tuttavia, se da un lato è vero che il processo di adozione dei rapporti di valutazione all'interno dell'IPCC è in parte di natura politica, dall'altro, la natura intergovernativa del Panel è stata fondamentale per garantire l'autorevolezza delle sue valutazioni e un impatto concreto sullo sviluppo di politiche climatiche[27]. Ad esempio, il primo rapporto dell'IPCC pubblicato nel 1990 è stato fondamentale per la creazione della Convenzione

20. Krige–Sarkar 2018.
21. Fischer 1997.
22. Roehrlich 2022; Council of Foreign Relations 2024.
23. Kimball–Bugos 2022.
24. Roehrlich 2022.
25. Vardy–Oppenheimer–Dubash et al. 2017; Bolin 2007.
26. Henderson 2007.
27. Vardy–Oppenheimer–Dubash et al. 2017.

Quadro delle Nazioni Unite sui Cambiamenti Climatici.

Un'altra critica rivolta all'IPCC riguarda potenziali conflitti di interesse all'interno dell'istituto[28]. Ad esempio, nel 2010, il presidente dell'IPCC Rajendra Pachauri fu criticato per presunti legami tra il centro di ricerca da lui diretto a Nuova Delhi e delle aziende interessate a promuovere determinate politiche sul cambiamento climatico. Queste accuse furono respinte dall'indagine che ne seguì, ma contribuirono all'adozione della policy sui conflitti di interesse dell'IPCC nel 2011. Oltre a stabilire misure precauzionali per prevenire conflitti di interesse tra la leadership dell'IPCC e organizzazioni private, questa policy tutela anche gli scienziati da influenze indebite dei governi.

5. Rilevanza dei modelli IAEA e IPCC per un istituto internazionale per la sicurezza dell'IA

I modelli IAEA e IPCC rappresentano due degli esempi più significativi di governance globale e, sotto determinati aspetti, possono fornire degli spunti utili ad arricchire l'attuale dibattito sulla governance dell'IA. Ad esempio, entrambi i modelli affrontano questioni legate alla valutazione e alla gestione del rischio, alla condivisione di conoscenze tecniche e alla cooperazione internazionale. Sia nel caso dell'IA che del cambiamento climatico, una delle sfide principali è gestire l'incertezza che caratterizza le modalità del manifestarsi di potenziali danni e l'entità del loro impatto. Allo stesso tempo, però, i problemi con cui devono confrontarsi l'AIEA e l'IPCC sono sostanzialmente diversi da quelli relativi all'IA. Mentre l'adattamento a processi esogeni è una priorità strategica della governance ambientale e il controllo della proliferazione nucleare per scopi militari è al centro degli sforzi dell'AIEA, l'obbiettivo fondamentale della governance dell'IA consiste nel garantire che le aziende che sviluppano e usano queste tecnologie lo facciano in modo sicuro e responsabile. Pertanto, se tracciare connessioni tra i modelli di governance in diversi ambiti politici può aiutare a pensare in modo creativo a quelle che potrebbero essere le funzioni di un istituto internazionale per la sicurezza dell'IA, è importante avere a mente che problemi distinti richiedono soluzioni altrettanto diverse.

Vari esperti del settore hanno sottolineato che il modello dell'AIEA potrebbe essere il punto di partenza per pensare a un'organizzazione che offre consulenza specialistica e coordinamento internazionale sul tema della sicurezza dell'IA[29]. La società OpenAI ha anche proposto di fondare "qualcosa di simile a un'AIEA per l'IA avanzata", capace di esaminare i modelli di IA prima che vengano messi in commercio, verificarne la conformità a determinati standard di sicurezza ed eventualmente anche imporre restrizioni sulla loro distribuzione[30]. La proposta di un organo di vigilanza globale sull'IA ispirato al modello dell'AIEA è stata appoggiata anche dal Segretario generale delle Nazioni Unite António Guterres[31].

Nonostante ciò, le critiche relative al doppio mandato dell'IAEA sollevano interrogativi simili nel caso di un istituto internazionale per la sicurezza dell'IA basato su un tale modello. Bisognerebbe stabilire, nel caso, se l'istituto possa svolgere attività di promozione e assistenza insieme a quelle di vigilanza. Inoltre, anche in questo caso, esiste il rischio che gli stakeholder più influenti strumentalizzino l'istituto per rafforzare la propria posizione al livello internazionale. Un ulteriore problema dell'analogia tra IA a nucleare è che la governance nucleare riguarda materiali che sono per natura scarsi e il cui utilizzo lascia tracce uniche e misurabili. Anche per questo motivo, lo sviluppo di tecnologie nucleari può essere efficacemente regolamentato attraverso misure di accesso controllato ai materiali, ispezione e approvazione. Nel caso dell'IA, una volta che un modello è addestrato, esso può essere integrato all'interno di varie applicazioni in maniera relativamente semplice e anonima[32]. L'analogia tra IA e nucleare, inoltre, riconduce il tema della sicurezza dell'IA all'interno

28. Schiermeier 2010, p. 596.
29. Marcus–Reuel 2023; Ho–Barnhart–Trager et al. 2023.
30. Altman–Brockman–Sutskever 2023.
31. Guterres 2023.
32. Afina–Lewis 2023.

di un contesto di rischio esistenziale. Un tale approccio concettuale, tuttavia, rischia di essere riduttivo[33]. Limitare l'IA all'interno di un contesto di rischio esistenziale, infatti, significherebbe ignorare la gamma di rischi che l'IA può porre all'autonomia e alla dignità individuale, alla prosperità e all'uguaglianza sociale, nonché all'integrità della sfera dell'informazione pubblica.

A complemento del dibattito sulla governance internazionale dell'IA, un'altra proposta avanzata di recente è quella di un Panel Internazionale sulla Sicurezza dell'IA (IPAIS) ispirato al modello dell'IPCC[34]. Questa proposta si fonda sul presupposto che, per sviluppare un regime regolatorio efficace per l'IA, è necessario che i decisori politici siano consapevoli delle tendenze più recenti e rilevanti nell'ambito della ricerca scientifica di settore. In questo senso, un istituto indipendente guidato da esperti con il compito di informare i governi sullo stato della ricerca scientifica sull'IA sarebbe strumentale a supportare lo sviluppo di un quadro di governance internazionale dell'IA. Oltre a valutare le ricerca in tema di capacità e i rischi dell'IA, l'IPAIS potrebbe anche sviluppare metodologie globalmente condivise per la rendicontazione e la valutazione dei sistemi di IA in modo analogo alla funzione svolta dalla Task Force dell'IPCC. Infine, l'IPAIS potrebbe coordinare una rete internazionale di istituti e organismi di ricerca sulla sicurezza dell'IA, contribuendo così al formarsi di una comunità scientifica specializzata e favorendo l'emergere di nuove collaborazioni e progetti di ricerca.

All'interno del dibattito sull'opportunità o meno di fondare l'IPAIS, è stato fatto notare che un tale istituto rappresenterebbe una piattaforma strategica per le aziende che sviluppano IA interessate ad influenzare i decisori politici[35]. Diversamente dal cambiamento climatico, fenomeno che può essere studiato da scienziati indipendenti in tutto il mondo, l'IA è una tecnologia sviluppata da un numero relativamente ristretto di aziende le quali tendono a non condividere pubblicamente la gran parte dei dati necessari a valutare i loro prodotti in modo indipendente. Per questi motivi, il design istituzionale di un IPAIS dovrebbe garantire una partecipazione del settore privato alle attività dell'Istituto che sia trasparente e orientata al pubblico interesse.

È evidente che i modelli dell'IPCC e della AIEA forniscono spunti potenzialmente utili per riflettere sull'assetto istituzionale e sulle funzioni di un'organizzazione internazionale per la sicurezza dell'IA. Tuttavia, è importante tenerne a mente anche i limiti. Come già visto, infatti, entrambe le istituzioni hanno avuto un impatto limitato, si sono dimostrate almeno in parte suscettibili ad interessi politici ed economici, e i modelli di governance che offrono non sono in grado di cogliere a pieno la natura sociotecnica dei sistemi di IA e le problematiche specifiche che ne derivano.

6. Primi passi verso l'istituzionalizzazione di funzioni di governance per la sicurezza dell'IA

Il Summit sulla sicurezza dell'IA ospitato dal Regno Unito nel novembre 2023 è stato probabilmente il primo tentativo esplicito di istituzionalizzare funzioni di governance per la sicurezza dell'IA su scala globale. L'obiettivo principale del Summit era stabilire un meccanismo di cooperazione internazionale per limitare i rischi legati alle forme di IA più avanzate. Sebbene dal Summit non siano emersi processi concreti ed attuabili per gestire tali rischi, un risultato comunque importante è stata la Dichiarazione di Bletchley. Firmata da 28 paesi e dall'Ue, la dichiarazione ha riconosciuto la necessità di un approccio globale allo studio dell'impatto che l'IA avrà sulla società. Tra le altre cose, i firmatari si sono impegnati a supportare il consolidamento di una comunità scientifica internazionale votata alla ricerca sulla sicurezza dell'IA.

Inoltre, il Summit sulla sicurezza dell'IA è stato pensato per essere un format continuativo. La seconda edizione del Summit si è svolta a maggio 2024 in Corea del Sud e la terza a Parigi nel febbraio 2025. In questo senso, il Summit potrebbe diventare esso stesso il primo meccanismo istituzionalizzato di cooperazione intergovernativa specificamente dedicato alla sicurezza dell'IA. A seguito dell'edizione coreana, i 27 paesi partecipanti e l'Ue hanno firmato la Dichiarazione ministeriale

33. Stewart 2023.

34. Suleyman–Cuellar–Bremmer et al. 2023.

35. Liu 2023.

di Seoul riaffermando la necessità di cooperare a livello internazionale per identificare e mitigare i rischi legati all'IA. Inoltre, una parte di questi paesi ha anche concordato di costituire una rete internazionale di istituti per la sicurezza dell'IA[36].

Un altro risultato della prima edizione del Summit è stata la nomina da parte degli Stati firmatari della Dichiarazione di Bletchley di un panel di esperti con il compito di redigere un report sullo stato della scienza dell'IA. Il report è stato pubblicato poco prima del Summit coreano con l'obbiettivo di proporre una lettura autorevole e ampiamente condivisa dei principali rischi connessi alle forme di IA più avanzata e di informare lo sviluppo di politiche nazionali e internazionali a riguardo[37].

Nel frattempo, sviluppi più concreti stanno prendendo forma a livello nazionale: in vista del primo Summit, il Regno Unito e gli Stati Uniti hanno creato degli istituti nazionali per la sicurezza dell'IA, l'UKAISI e l'USAISI.

L'UKAISI è stato creato per rispondere alla necessità di garantire che i rischi posti dalle forme di IA più avanzate siano valutati in modo indipendente e nel pubblico interesse. L'istituto ha un triplice mandato: (a) sviluppare metodologie per la valutazione tecnica delle capacità potenzialmente dannose dei modelli IA; (b) svolgere ricerche sul tema della sicurezza dell'IA per supportare nuove soluzioni di governance; (c) facilitare la condivisione di informazioni tra decisori politici, aziende, ricercatori e società civile sia a livello nazionale che internazionale. I risultati delle valutazioni condotte dall'Istituto non condizionano il rilascio o la vendita dei modelli IA valutati come rischiosi, ma hanno lo scopo di supportare i processi decisionali sia al livello politico che commerciale. L'UKAISI, inoltre, pubblica le metodologie di valutazione che sviluppa affinché possano essere riutilizzate ed eventualmente migliorate da altri ricercatori. Sebbene sia ancora agli albori della sua attività, l'istituto è stato in parte già criticato per la dubbia efficacia delle sue valutazioni e per la mancanza di accesso ai modelli di IA più recenti e avanzati[38].

Il mandato dell'USAISI corrisponde in parte a quello del suo omologo britannico. È incaricato dal governo americano di (a) sviluppare strumenti e linee guida per valutare le capacità potenzialmente dannose dei modelli di IA; (b) facilitare la condivisione di informazioni e il coordinamento con le controparti nazionali e internazionali; (c) produrre linee guida per lo sviluppo e l'applicazione di regolamenti specifici per l'IA. Nel febbraio 2024, il Segretario al Commercio degli Stati Uniti ha annunciato che l'USAISI sarà supportato dal Consorzio sulla Sicurezza dell'IA. Il Consorzio è una piattaforma che riunisce più di 200 aziende attive nel settore dell'IA, organi pubblici, ricercatori e organizzazioni della società civile per stabilire uno spazio di condivisione di dati e conoscenza e offrire input utili al lavoro di ricerca e valutazione dell'USAISI.

Da una prospettiva funzionale, quindi, gli istituti per la sicurezza dell'IA del Regno Unito e degli Stati Uniti sembrano essere almeno parzialmente ispirati alle caratteristiche proprie dei modelli IAEA e IPCC. Ad esempio, i due istituti svolgono un ruolo chiave nel facilitare la condivisione di conoscenze scientifiche e tecniche. Sviluppano metodologie per valutare l'impatto negativo dell'IA, come l'IAEA fa nel contesto dell'uso militare dell'energia nucleare. Supportano la cooperazione e la collaborazione tra una vasta gamma di parti interessate con l'obiettivo di stimolare il progresso scientifico e l'innovazione tecnologica. Infine, contribuiscono allo sviluppo di quadri di governance pubblicando analisi indipendenti e autorevoli sullo stato dell'arte della ricerca sull'IA.

7. Potenziali funzioni di un istituto internazionale per la sicurezza dell'IA

Gli istituti nazionali per la sicurezza dell'IA del Regno Unito e degli Stati Uniti rappresentano dei passi avanti importanti per lo sviluppo di capacità di valutazione e controllo dei rischi dell'IA da parte delle istituzioni pubbliche. Tuttavia, il carattere transnazionale di tali rischi rende necessario stabilire meccanismi di coordinamento e controllo anche a livello internazionale. Una delle possibili soluzioni a riguardo è la creazione di un istituto internazionale specializzato, similmente a quanto avvenuto nelle aree della governance ambientale e nucleare. Per quanto vi siano opinioni contrastanti

36. DSIT 2024-A; DSIT 2024-B.

37. Bengio–Mindermann–Privitera 2024.

38. Narayanan–Kapoor 2024.

sull'opportunità di creare un organo del tutto nuovo piuttosto che utilizzare strutture e processi esistenti, è comunque utile riflettere sul ruolo e sulle funzioni che un tale istituto potrebbe eventualmente svolgere.

Sulla base di quanto visto nel caso dell'IPCC e dell'AIEA, e considerando gli esempi dell'UKAISI e dell'USAISI al livello nazionale, è possibile articolare il profilo funzionale di un istituto internazionale per la sicurezza dell'IA all'interno di tre categorie tematiche generali: (a) ricerca e cooperazione, (b) audit e verifiche di conformità dei modelli di IA e (c) supporto tecnico per la definizione di quadri di governance dell'IA. Di seguito si propone un elenco non esaustivo di funzioni specifiche rientranti in ciascuna di queste categorie.

7.1. Ricerca e cooperazione

Le principali funzioni di ricerca e cooperazione di un istituto internazionale per la sicurezza dell'IA comprendono: a) la valutazione dello stato della ricerca scientifica sulla sicurezza dell'IA e l'identificazione dei rischi dell'IA attuali e futuri, del loro potenziale impatto sulla società, e dell'efficacia delle soluzioni proposte per gestirli; b) il supporto della ricerca scientifica sulla sicurezza dell'IA attraverso l'identificazione di aree di ricerca di importanza strategica e l'erogazione di incentivi di natura tecnica e finanziaria a sostegno di nuovi progetti di ricerca in queste aree; c) il supporto della cooperazione scientifica internazionale in tema di sicurezza dell'IA fungendo da piattaforma di coordinamento per ricercatori e scienziati, e incentivando la diffusione di conoscenza e competenze tecniche per migliorare la comprensione dei rischi dell'IA da parte di coloro che sviluppano e usano queste tecnologie; d) il supporto tecnico e l'assistenza necessaria a garantire l'accesso a risorse computazionali e dataset per l'addestramento dei modelli di IA da parte delle nazioni in via sviluppo; e) il coordinamento delle attività degli istituti nazionali per la sicurezza dell'IA, incluso il supporto all'uso di metodologie standardizzate e condivise per la valutazione dei rischi legati all'IA.

7.2. Audit e verifiche di conformità dei modelli di IA

Un'altra importante area funzionale di un istituto internazionale per la sicurezza dell'IA riguarda la valutazione tecnica dei modelli di IA. Tra le principali funzioni rientranti in questa categoria vanno menzionati: a) lo sviluppo di processi e metodologie condivisi a livello internazionale per valutare la sicurezza dei modelli di IA e mitigarne le capacità potenzialmente dannose; b) la valutazione dei modelli di IA più avanzati – esempi di tecniche di valutazione particolarmente diffuse sono il *red-teaming*, le *human uplift evaluations*, e le *AI agent evaluations*; c) la definizione di standard di sicurezza e *best practices* per lo sviluppo, l'uso e l'acquisizione di tecnologie IA; d) la verifica della conformità delle policy di sicurezza adottate dalle principali aziende che sviluppano IA rispetto a standard di sicurezza predefiniti e condivisi; e) la pubblicazione gratuita di metodologie per valutare i modelli IA in modo da contribuire alla diffusione di benchmark per la sicurezza dell'IA al livello internazionale.

7.3. Supporto tecnico per la definizione di quadri di governance dell'IA

L'ultima categoria funzionale di un istituto internazionale per la sicurezza dell'IA identificata da questa analisi comprende funzioni di supporto allo sviluppo e consolidamento di quadri di governance internazionale per la sicurezza dell'IA. Ciò include: a) la condivisione di competenze tecniche e informazioni utili a supportare lo sviluppo di politiche per la sicurezza dell'IA, per esempio sintetizzando le ricerche condotte dagli istituti nazionali per la sicurezza dell'IA e condividendone i risultati con una rete di decisori politici nazionali e internazionali per supportare lo sviluppo di soluzioni di governance innovative; b) funzioni di consulenza tecnica e strategica per facilitare lo sviluppo e l'applicazione di norme per la sicurezza dell'IA da parte dei regolatori nazionali.

8. Conclusione

Partendo dalla constatazione della necessità di formalizzare a livello internazionale processi per identificare e gestire le capacità potenzialmente dannose dell'IA, questo articolo propone una riflessione sulle possibili funzioni di un istituto internazionale per la sicurezza dell'IA. Sulla base dell'analisi dei modelli di governance internazionale esistenti in settori adiacenti a quello dell'IA e delle funzioni degli istituti nazionali per la sicurezza dell'IA recentemente costituiti nel Regno Unito e negli Stati Uniti, l'articolo identifica tre categorie

generali di funzioni che potrebbero essere svolte da un istituto internazionale per la sicurezza dell'IA: a) ricerca tecnica e cooperazione, b) audit e verifiche di conformità dei modelli di IA e c) supporto tecnico per la definizione di quadri di governance dell'IA.

L'analisi presentata in questo articolo fornisce una base concettuale per sviluppare ulteriori ricerche in almeno tre ambiti complementari. In primo luogo, e con riferimento allo studio comparato dei modelli dell'IPCC e l'IAEA, sarebbe utile studiarne non solo le funzioni principali e l'impatto ottenuto, ma anche il loro design istituzionale, inclusi i modelli di finanziamento, di *membership*, le strutture di governance interna e i processi che regolano i rapporti con gli stakeholders. In secondo luogo, ulteriori ricerche di natura comparata potrebbero includere una gamma più ampia di istituzioni come la *Financial Action Taskforce* (FATF) e l'Organizzazione Europea per la Ricerca Nucleare (CERN). Inoltre, posto che diversi paesi stanno costituendo istituti nazionali per la sicurezza dell'IA – inclusi Giappone, Singapore, Canada, India, Cina e Corea del Sud – potrebbe essere interessante analizzare quali sono gli elementi in comune tra questi ultimi, l'UKAISI e l'USAISI. Infine, è importante considerare che ci sono diverse opzioni per stabilire processi istituzionalizzati per la sicurezza dell'IA a livello internazionale. Queste includono la creazione *ex novo* di un istituto internazionale per la sicurezza dell'IA, il consolidamento di un network di istituti nazionali per la sicurezza dell'IA, nonché l'attribuzione di nuove competenze e poteri a istituzioni internazionali già esistenti come l'ONU e l'OCSE. Valutare i pro e i contro di ciascuna opzione rappresenta anch'esso un importante ambito di ricerca complementare all'analisi svolta in questo articolo.

Bibliografia

Y. Afina, P. Lewis (2023), *The nuclear governance model won't work for AI*, Chatham House – International Affairs Think Tank, 2023

S. Agrawala (1998-a), *Context and Early Origins of the Intergovernmental Panel on Climate Change*, in "Climatic Change", vol. 39, 1998

S. Agrawala (1998-b), *Structural and Process History of the Intergovernmental Panel on Climate Change*, in "Climatic Change", vol. 39, 1998

S. Altman, G. Brockman, I. Sutskever (2023), *Governance of superintelligence*, OpenAI, 2023

Y. Bengio, S. Mindermann, D. Privitera et al. (2024), *International Scientific Report on the Safety of Advanced AI: Interim Report*, DSIT 2024/009, 2024

B. Bolin (2007), *A History of the Science and Politics of Climate Change: The Role of the Intergovernmental Panel on Climate Change*, Cambridge University Press, 2007

R. Bommansani, D.A. Hudson, E. Adeli et al. (2022), *On the Opportunities and Risks of Foundation Models*, arXiv, 2022

A. Booth (2016), *EVIDENT Guidance for Reviewing the Evidence: a compendium of methodological literature and websites*, Working paper, 2016

R. Brown, J. Kaplow (2014), *Talking Peace, Making Weapons: IAEA Technical Cooperation and Nuclear Proliferation*, in "Journal of Conflict Resolution", vol. 58, 2014, n. 3

CMA (2024), *CMA AI Strategic Update*, UK Competition and Markets Authority, 2024

Council of Europe (2024), *Framework Convention on Artificial Intelligence and HumanRights, Democracy and the Rule of Law*, Council of Europe Treaty Series - No. 225, 2024

Council of Foreign Relations (2024), *Timeline: North Korean Nuclear Negotiations*, Council on Foreign Relations, 2024

K. De Pryck, M. Hulme (eds.) (2022), *A Critical Assessment of the Intergovernmental Panel on Climate Change*, Cambridge University Press, 2022

DSIT (2024-a), *Seoul Ministerial Statement for Advancing AI Safety, Innovation, and Inclusivity: AI Seoul Summit 2024*, UK Department for Science, Innovation, and Technology, 2024

DSIT (2024-b), *Seoul Intent Toward International Cooperation on AI Safety Science, AI Seoul Summit 2024 (Annex)*, UK Department for Science, Innovation, and Technology, 2024

DSIT (2023), *Introducing the AI Safety Institute*, UK Department for Science, Innovation, and Technology, 2023

D. Fischer (1997), *History of the International Atomic Energy Agency: The First Forty Years*, International Atomic Energy Agency, 1997

GPAI (2023), *State-of-the-art Foundation AI Models Should be Accompanied by Detection Mechanisms as a Condition of Public Release*, Report, Global Partnership on AI, 2023

A. Guterres (2023), *Secretary-General Urges Security Council to Ensure Transparency, Accountability, Oversight, in First Debate on Artificial Intelligence*, United Nations, 2023

I. Habli (2023), *On the Meaning of AI Safety*, University of York, 2023

D. Henderson (2007), *Unwarranted Trust: A Critique of the IPCC Process*, in "Energy & Environment", vol 18, 2007, n. 7-8

J. Hendrix (2023), *Exploring Global Governance of Artificial Intelligence*, Tech Policy Press, 2023

L. Ho, J. Barnhart, R. Trager et al. (2023), *International Institutions for Advanced AI*, arXiv, 2023

IAEA (1956), *The Statute of the IAEA*, International Atomic Energy Agency, 1956

ICO (2023), *Guidance on AI and data protection*, UK Information Commissioner's Office, 2023

A. Jobin, M. Ienca, E. Vayena (2019), *The global landscape of AI ethics guidelines*, in "Nature", 2019

C.F. Kerry, J.P. Meltzer, A. Renda et al. (2021), *Strengthening International Cooperation on AI*, Brookings, 2021

D. Kimball, S. Bugos (2022), *Timeline of the Nuclear Nonproliferation Treaty (NPT)*, Arms Control Association, 2022

J. Krige, J. Sarkar (2018), *US technological collaboration for nonproliferation: Key evidence from the Cold War*, in "The Nonproliferation Review", vol. 25, 2018, n. 3-4

D. Leslie (2019), *Understanding artificial intelligence ethics and safety*, The Alan Turing Institute, 2019

D. Leslie, C. Burr, M. Aitken et al. (2021), *AI, human rights, democracy and the rule of law: A primer prepared for the Council of Europe*, The Alan Turing Institute, 2021

L. Liu (2023), *Letter: Setting rules for AI must avoid regulatory capture by Big Tech*, in "Financial Times", 27 October 2023

M. Mäntymäki, M. Minkkinen, T. Birkstedt, M. Viljanen (2022), *Defining organizational AI governance*, in "AI and Ethics", vol. 2, 2022

G. Marcus, A. Reuel (2023), *The world needs an international agency for artificial intelligence, say two AI experts*, in "The Economist", 2023

D. Milmo (2023), *AI risk must be treated as seriously as climate crisis, says Google DeepMind chief*, in "The Guardian", 24 October 2023

A. Narayanan, S. Kapoor (2024), *AI Safety is not a model property*, AI Snake Oil, 2024

NIST (2023-A), *U.S. Artificial Intelligence Safety Institute*, 2023

NIST (2023-B), *Artificial Intelligence Risk Management Framework (AI RMF)*, 2023

OECD (2023), *G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI*, OECD Publishing, 2023

OECD (2019), *OECD AI Principles Overview*, Organisation for Economic Cooperation and Development, 2019

Prime Minister's Office (2023), *UK to host first global summit on Artificial Intelligence*, 2023

H. Roberts, E. Hine, M. Taddeo, L. Floridi (2023), *Global AI governance: Barriers and pathways forward*, in "International Affairs", vol. 100, 2023, n. 3

H. Roberts, M. Ziosi, C. Osborne (2023), *A Comparative Framework for AI Regulatory Policy*, Ceimia, 2023

E. Roehrlich (2022), *Inspectors for Peace*, Johns Hopkins University Press, 2022

Q. Schiermeier (2010), *IPCC flooded by criticism*, in "Nature", vol. 463, 2010

S. Steinmo, K. Thelen, F. Longstreth (eds.) (1992), *Structuring Politics: Historical Institutionalism in Comparative Analysis*, Cambridge University Press, 1992

I.J. Stewart (2023), *Why the IAEA model may not be best for regulating artificial intelligence,* in "Bulletin of the Atomic Scientists", 2023

M. Suleyman, M.-F. Cuéllar, I. Bremmer et al. (2023), *Proposal for an International Panel on Artificial Intelligence (AI) Safety (IPAIS): Summary*, Carnegie Endowment for International Peace, 27 October 2023

M. Suleyman, E. Schmidt (2023), *Mustafa Suleyman and Eric Schmidt: We need an AI equivalent of the IPCC*, in "Financial Times", 2023

The American Presidency Project (2023), *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, 2023

C. Thomas, H. Roberts, J. Mökander et al. (2024), *The case for a broader approach to AI assurance: addressing 'hidden' harms in the development of artificial intelligence*, in "AI & SOCIETY", 16 May 2024

UN - AI Advisory Body (2023), *Final Report - Governing AI for Humanity*, United Nations, 2023

UN - Office for Disarmament Affairs (1970), *Treaty on the Non-Proliferation of Nuclear Weapons (NPT)*, United Nations, 1970

M. Vardy, M. Oppenheimer, N.K. Dubash et al. (2017), *The Intergovernmental Panel on Climate Change: Challenges and Opportunities*, in "Annual Review of Environment and Resources", vol. 42, 2017

M. Veale, K. Matus, R. Gorwa (2023), *AI and Global Governance: Modalities, Rationales, Tensions*, in "Annual Review of Law and Social Sciences", vol. 19, 2023

L. Weiss (2017), *Safeguards and the NPT: Where our current problems began*, in "Bulletin of the Atomic Scientists", vol. 73, 2017

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0206 • articolo sottoposto a peer review • pubblicato in anteprima il 4 mar. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Antonio Manganelli

Decentralized Autonomous Organization, blockchain e impresa: considerazioni giuridico-economiche

Le *Decentralized Autonomous Organizations* (DAO) sono organizzazioni economiche fondate su *Distributed Ledger Technology* (DLT) che, avvalendosi di software di automatizzazione dei processi decisionali e amministrativi, agevolano la partecipazione dei soggetti coinvolti nell'organizzazione imprenditoriale. L'articolo indaga in chiave di analisi economica del diritto il funzionamento delle DAO e analizza in termini comparati le nascenti e parziali discipline giuridiche esistenti, con un duplice obiettivo: in primo luogo, esaminare se e in che misura la tecnologia *blockchain* possa risolvere alcuni dei problemi di governance che tipicamente emergono nelle organizzazioni caratterizzate da un'ampia base partecipativa; in secondo luogo, contribuire alla letteratura sulle forme legalmente riconosciute di organizzazione imprenditoriale, fornendo una disamina su potenzialità e limiti connessi all'automazione dei processi gestori e decisionali resi possibili dalle applicazioni su *blockchain*.

DAO – Decentralizzazione – Organizzazione imprenditoriale – Corporate governance – Token

A law and economics look to Decentralized Autonomous Organization, blockchain and business organisation

Decentralized Autonomous Organizations (DAOs) are economic organizations based on Distributed Ledger Technology (DLT) that make use of software to automate decision-making and administrative processes, thus facilitating the participation of stakeholders in the business organization. This essay investigates from an economic analysis of law viewpoint the functioning of DAOs and analyses in comparative terms the legal disciplines that have started to develop. This analysis has a twofold objective: first, to examine whether and to what extent blockchain technology can address some of the governance problems that typically arise in organizations with a broad participatory base; second, to contribute to the academic reflection on legally recognized forms of entrepreneurial organization by assessing pros and cons related to the automation of management and decision-making made it possible by blockchain applications.

DAOs – Decentralisation – Business organization – Corporate governance – Tokens

L'Autore è professore a contratto di Diritto e politiche della concorrenza, Scuola di economia e management dell'Università degli Studi di Siena

Sommario: 1. Introduzione. – 2. Un inquadramento tecnico-economico. – 3. Prime riflessioni giuridiche e di analisi economica del diritto. – 3.1. Responsabilità illimitata. – 3.2. Rappresentanza. – 3.3. *Corporate governance*. – 3.4. *Token* di partecipazione. – 4. L'evoluzione della disciplina giuridica delle DAO in Ue e USA. – 5. Breve conclusione.

1. Introduzione

Le *Decentralized Autonomous Organizations* (DAO) sono organizzazioni fondate su *Decentralized Ledger Technologies* (DLT) o sistemi di *blockchain* le quali, avvalendosi di software che automatizzano i processi decisionali e amministrativi, mirano ad agevolare la partecipazione dei soggetti coinvolti nei processi imprenditoriali[1]. Le DAO funzionano grazie alla combinazione di tre elementi fondamentali: (i) *smart contract*, ossia programmi auto-eseguibili che definiscono le regole dell'organizzazione e gestiscono automaticamente le risorse; (ii) gettoni virtuali (*token*) di governance, che attribuiscono "diritti di voto" ai detentori al fine di partecipare alle decisioni dell'organizzazione, e.g., l'allocazione di fondi, l'approvazione di nuovi progetti o modifiche alla struttura della DAO; (iii) i membri/partecipanti all'organizzazione, coloro cioè che hanno acquisito (i.e., acquistato o guadagnato) *token*.

Le DAO rappresentano uno degli sviluppi giuridicamente più interessanti della c.d. finanza decentralizzata (DeFi), ossia quel nascente ecosistema di servizi finanziari, che opera senza la necessità di intermediari tradizionali, offrendo strumenti finanziari (prestiti, investimenti, scambi di criptovalute, assicurazioni, ecc.) attraverso, appunto, protocolli e piattaforme distribuite, così come *smart contract* che eseguono automaticamente operazioni secondo regole predefinite[2].

Le DAO hanno fatto primariamente il proprio ingresso nel dibattito giuridico-economico a seguito del malfunzionamento relativo al "Project DAO" verificatosi nel 2016, uno *smart contract* eseguito su Ethereum, programmato per assolvere le funzioni di un fondo di *venture capital*. Questo programma informatico era ideato per consentire a qualsiasi possessore munito dei relativi gettoni virtuali di proporre un progetto da finanziare attraverso votazione digitale decentralizzata. Il possessore di tali *token* aveva la possibilità di partecipare alla votazione sui progetti candidati e avrebbe ricevuto ricompense proporzionali alla redditività degli stessi. Poco dopo aver raccolto un ammontare di criptovalute ether (ETH) pari a 150 milioni di dollari tramite una vendita di *token*, un membro ha sfruttato una vulnerabilità nel codice per sottrarre risorse alla DAO con un valore di circa 60 milioni di dollari. Ciò ha indotto i fondatori ad operare una forzatura nella programmazione della *blockchain* Ethereum per restituire i fondi ai precedenti detentori, violando così il principio di immutabilità e resistenza della *blockchain* sottostante, cristallizzato nel motto "*code is law*" ("il codice di programmazione è legge")[3].

1. Per un inquadramento generale, si veda: Rodi–Santoro 2024; Laudonio 2023; per la letteratura precedente, si rimanda a: Carrière–de Luca–de Mari et al. 2023; Cuocci–Lops–Motti 2021; Annunziata–Chisari–Amendola 2023 per un quadro normativo sulle cripto-attività elettroniche.
2. Capelli 2023; Carrière 2023; Lemma 2023; Piselli 2019.
3. Tale forzatura è consistita in una c.d. *hard fork*, ossia un aggiornamento radicale che può rendere valide o non valide le transazioni e i blocchi precedenti, e richiede che tutti i nodi di una rete si aggiornino a una versione

Ad oggi, progetti di DAO sono stati avviati principalmente negli Stati Uniti da comunità relativamente ristrette di convinti sostenitori della DLT (*blockchain*), i quali sottolineano significativi miglioramenti rispetto ai metodi tradizionali di gestione dell'impresa, e.g., in termini di (i) trasparenza, in quanto tutte le transazioni e decisioni sono registrate sulla *blockchain* e sono verificabili da chiunque; (ii) decentramento, in quanto si elimina il bisogno di una leadership centralizzata, distribuendo il potere decisionale tra tutti i partecipanti; e (iii) efficacia ed efficienza operativa, in quanto le operazioni sono automatizzate tramite *smart contract*, che riducono costi di transazione e di gestione.

Tuttavia, le DAO al momento sono scarsamente diffuse come strumento di organizzazione imprenditoriale, in ragione delle loro problematicità operative ma anche dell'incertezza giuridica inerente alla loro natura e alla natura delle relazioni economiche che si instaurano esternamente all'organizzazione. A questo proposito, alcuni autori hanno infatti evidenziato come sia improbabile che le stesse, almeno allo stato attuale, si possano diffondere agevolmente nell'economia reale[4].

Questo articolo vuole approfondire tali questioni, cercando di comprendere il potenziale ruolo delle DAO nel futuro dell'organizzazione imprenditoriale e le inevitabili interazioni con il contesto giuridico-economico circostante. Il punto chiave di tale analisi è la comprensione del ruolo del diritto nel disciplinare lo status di tali organizzazioni nonché l'eventuale bisogno di nuove disposizioni regolatorie per rendere le DAO un effettivo strumento di organizzazione imprenditoriale alternativo a quelli tradizionalmente adoperati.

L'ambizione di questo approfondimento è duplice. In primo luogo, esaminare se e in che misura la tecnologia *blockchain* possa risolvere i problemi di corporate governance che tipicamente emergono nelle organizzazioni caratterizzate da un'ampia base partecipativa. In secondo luogo, contribuire alla letteratura sulle forme legalmente riconosciute di organizzazione imprenditoriale, fornendo una disamina su potenzialità e limiti connessi all'automazione dei processi gestori e decisionali resi possibili dalle applicazioni su *blockchain*.

2. Un inquadramento tecnico-economico

Una DAO, nella forma attualmente più comune e semplice, può essere intesa come un meccanismo organizzativo derivante dall'accordo di due o più parti, che è disciplinato e implementato automaticamente da *smart contract*, ossia programmi informatici eseguiti tramite DLT che consentono l'esecuzione automatica di regole consequenziali e binarie preimpostate (i.e., se A allora B).

In questo contesto tecnico-economico, ogni fase dell'esecuzione, come il trasferimento di un bene, l'acquisizione di informazioni da una fonte esterna e così via, viene registrata in modo indelebile e pubblico sul registro DLT. Ciò significa che le attività eseguite attraverso uno *smart contract*, una volta registrate sulla *blockchain*, non possono essere alterate o cancellate[5]. La sottostante infrastruttura DLT/*blockchain*, infatti, è un registro crittografico decentralizzato ripetutamente validato, costituito da una rete di nodi che fornisce una registrazione cronologica permanente di tutte le modifiche precedenti.

Oltre alle garanzie di trasparenza e protezione, il principale vantaggio degli *smart contract* è rappresentato dalla sostanziale riduzione dei costi legati alla creazione, all'esercizio e alla verifica dei diritti nel contesto delle relazioni commerciali[6]. Di conseguenza, gli individui che partecipano a una DAO non hanno bisogno di affidarsi a intermediari e sistemi esterni per controllare e

più recente. In particolare, tale operazione impone agli operatori dei nodi d'accordo all'implementazione della stessa di aggiornarsi all'ultima versione del protocollo. Pertanto, i nodi che non implementano la *hard fork* continueranno nei fatti a mantenere un registro che sarà diverso e altro rispetto a quello "rinnovato" a seguito della *hard fork*. Sul punto si veda: Allen 2020; DuPont 2017.

4. Schuster 2021.

5. Doria–Bassan–Rabitti et al. 2024; Borgogno 2018; Raskin 2017.

6. Si veda Yermack 2017. In una fase del tutto embrionale di sviluppo della tecnologia DLT, l'Autore già collocava l'impatto della stessa nell'ambito della riduzione di costi di transazione che caratterizzano le dinamiche economiche sottostanti all'organizzazione societaria.

gestire i beni dell'organizzazione, direttamente o indirettamente[7].

Pertanto, secondo i sostenitori delle DAO, non vi sarebbe alcuna necessità di ricorrere a formalità giuridiche per disciplinare i rapporti tra fondatori e partecipanti. Si presume infatti che i possessori dei *token*, avendo la possibilità di controllare in anticipo il codice e le istruzioni sottostanti alla DAO, non dovrebbero fare altro che affidarsi all'automatica esecuzione del programma informatico[8].

La partecipazione in una DAO avviene infatti mediante il conferimento di *token* ai partecipanti la cui costituzione e il cui traffico è interamente operato tramite *blockchain*. Questi gettoni digitali possono essere ottenuti come corrispettivo per un controvalore o assegnati gratuitamente dal protocollo informatico a soggetti che hanno preso parte allo sviluppo della DAO. Gli stessi possono poi essere scambiati sul mercato secondario operante su DLT e fornire diritti specifici di carattere patrimoniale e amministrativo[9]. Per esempio, alcune DAO conferiscono ai membri il diritto a una parte dei profitti e delle perdite di un'organizzazione; altre forniscono ai loro membri il diritto di accedere o gestire le risorse o i servizi che l'organizzazione negozia e gestisce.

La governance delle DAO assume forme meno gerarchiche rispetto alle forme societarie tradizionali, distribuendo e decentralizzando il potere decisorio e gestionale[10]. I diritti di voto vengono esercitati attraverso i *token* che vengono distribuiti agli utenti dallo *smart contract*, nonché agli sviluppatori e agli investitori che hanno sostenuto la nascita del progetto. Le decisioni assunte dall'organizzazione dipendono solitamente dal consenso di gruppo o dal voto della maggioranza dei possessori di *token*, in omaggio ad un principio di partecipazione diretta alla vita dell'organizzazione.

Nella sua essenza, la tassonomia delle DAO può essere concettualizzata come uno spettro che comprende una gamma diversificata di configurazioni. Questo spettro ricomprende sia entità in cui una moltitudine di funzioni (tra cui il processo decisionale e le interazioni con i detentori di *token*) sono algoritmicamente automatizzate, sia strutture relativamente più semplici caratterizzate dall'uso di codice principalmente a scopo di rendicontazione, come esemplificato dal protocollo Bitcoin.

Le DAO con un minore livello di automazione algoritmica contribuiscono ad attenuare alcune rigidità organizzative che caratterizzano gli *smart contract*. Si tratta delle cosiddette "DAO partecipative", in cui il software viene impiegato per aggregare i voti o le preferenze espresse dai membri su base continua nonché per tradurre tali informazioni in decisioni secondo le regole stabilite dal protocollo. Questo tipo di cripto-organizzazione è comunemente utilizzato per intraprendere attività imprenditoriali tradizionali – come operazioni di *venture capital*.

Il programma informatico inoltre viene utilizzato per raccogliere e coordinare le interazioni tra i possessori di *token*. Affidandosi ad una DAO, i fondatori, che di solito sono gli sviluppatori iniziali del protocollo basato su *smart contract*, possono coinvolgere nel processo decisionale gli utenti e i sostenitori iniziali del progetto. Gli sviluppatori di queste DAO mantengono generalmente un potere di controllo gestorio che consente loro di modificare le regole alla base del rapporto organizzativo stesso.

L'alternativa più radicale, allo stato in gran parte teorica, è quella delle "DAO algoritmiche", in cui le scelte gestorie sono interamente delegate *ex ante* all'algoritmo sottostante. Le DAO algoritmiche sono concepite per funzionare autonomamente, eseguendo azioni in base a specifici input o cambiamenti nelle condizioni esterne (ad esempio, il prezzo di una criptovaluta, condizioni di mercato, ecc.). Poiché gli algoritmi prendono le decisioni operative principali, c'è una ridotta necessità di votazioni o di interventi da parte della comunità per il funzionamento quotidiano[11]. Queste organizzazioni offrono, in teoria, efficienza e

7. Rigazio 2021; Davola–Pardolesi 2020; Poncibò 2020.
8. Rodrigues 2019; Wright–De Filippi 2015.
9. Rohr–Wright 2019.
10. Gola–Cappa–Fiorenza et al. 2023.
11. A questo proposito si deve osservare che, anche se le DAO algoritmiche rappresentano un estremo di decentralizzazione, esiste comunque il rischio che il processo di progettazione e impostazione degli algoritmi, controllato

imparzialità nella governance ancor più accentuate rispetto alle "DAO partecipative", esse presentano, tuttavia, grandi sfide legate alla gestione di situazioni di "crisi", sia derivanti dal malfunzionamento dei software[12], sia derivanti dalla mancanza di flessibilità in situazioni non previste e prevedibili *ex ante*.

In sintesi, i fautori delle DAO (sia partecipative, sia algoritmiche) ritengono che questo nuovo modello di organizzazione goda di significative efficienze operative rispetto ad altre forme organizzative[13]. Non a caso, le DAO sono in grado di riunire e re-distribuire agevolmente beni espressi in forma di cripto-attività, di implementare schemi di voto digitale rapidi e a basso costo, di utilizzare procedure di monitoraggio trasparenti che proteggono gli asset e di ridurre la necessità di un controllo continuo per contrastare frodi o altri abusi da parte di soggetti interni ed esterni all'organizzazione.

Tuttavia, i suddetti vantaggi si accompagnano ad un'architettura organizzativa rigida che, qualora contempli una forte dispersione della base partecipativa tra una miriade di possessori di *token*, potrebbe rendere quasi impossibile modificare il modello di business o il funzionamento interno per rispondere a nuove dinamiche di mercato. Questo elemento può rappresentare un grave ostacolo, soprattutto per le imprese in una fase iniziale di sviluppo, quando sono spesso necessari continui aggiustamenti allo schema di impresa e al quadro organizzativo[14].

Nella misura in cui le DAO sono implementate su una *blockchain* pubblicamente accessibile, la trasparenza e la possibilità di controllo dovrebbero essere significativamente più elevate rispetto alle società tradizionali. Utilizzando un sistema di voto basato su *blockchain*, i membri dovrebbero essere in grado di verificare crittograficamente i risultati delle votazioni dei membri (ad esempio, in assenza di voto segreto, chi ha votato e come) e se le identità dei titolari di *token* sono correlate con gli indirizzi utilizzati per il voto. Le decisioni dei membri della DAO sono aperte alla verifica pubblica da parte di tutti i membri dell'organizzazione (e potenzialmente anche del pubblico), contribuendo a garantire il rispetto delle regole procedurali per il processo decisionale e a evitare i rischi di errori di conteggio dei voti.

Nelle intenzioni dei loro promotori, le DAO presenterebbero il potenziale di superare la concentrazione del potere gestorio nelle mani del consiglio di amministrazione nelle società per azioni. Tale risultato sarebbe possibile tramite l'agevole coinvolgimento dei detentori di *token* nelle scelte gestionali dell'organizzazione.

Infine, le DAO sono spesso descritte come strumenti utili per rimediare alle problematiche di appropriazione indebita o uso improprio dei fondi comuni. A differenza delle organizzazioni tradizionali, le DAO sono governate secondo regole rigide definite nel codice degli *smart contract*. Ciò dovrebbe consentire di strutturare le dinamiche aziendali in modo più deterministico, con un codice che dettaglia le regole in base alle quali i partecipanti e i soggetti esterni possono interagire.

3. Prime riflessioni giuridico-economiche e di analisi economica del diritto

Uno degli aspetti principali da analizzare con riferimento alle DAO è il rapporto esistente tra le loro peculiarità tecnologiche, i rischi di carattere economico che queste possono creare in capo ai loro

da una piccola élite di sviluppatori o detentori di *token*, potrebbe introdurre "forme occulte di controllo centralizzato". Wright 2021.

12. Gli *smart contracts* sono il cuore operativo delle DAO, poiché gestiscono automaticamente regole e transazioni senza intervento umano. Tuttavia, sono vulnerabili a errori nel codice o a "bug". Se un contratto intelligente contiene una falla, può essere sfruttato da hacker o malintenzionati, causando gravi perdite di fondi. Come detto, un celebre esempio è stato The DAO del 2016, che è stata violata a causa di una vulnerabilità nello *smart contract*, portando alla perdita di milioni di dollari in Ethereum.
13. E per questo motivo, sia tuttora già utilizzato per gestire il traffico di centinaia di beni con un valore complessivo nell'ordine delle centinaia di milioni di dollari.
14. Martino–Ringe 2024. Gli Autori propongono un ampliamento del quadro delle esternalità derivanti dall'impiego della tecnologia DLT, che andrebbero a bilanciare in negativo le maggiori efficienze gestionali su cui si è focalizzata la letteratura più risalente.

partecipanti e le soluzioni giuridiche che potrebbero porre (parziale) rimedio agli stessi[15].

3.1. Responsabilità illimitata

Con riferimento allo status giuridico delle DAO, è utile operare una distinzione tra DAO registrate e non registrate. Le prime sono costituite come società di capitali in conformità al quadro giuridico del paese in cui operano. Le seconde si basano esclusivamente su una cooperazione informale tra i partecipanti, operata e resa possibile dal sottostante *smart contract*.

Come anticipato nella descrizione tecnico-economica, secondo il mantra "il codice è legge", le DAO sono state ideate con l'ambizione di essere totalmente autonome da ogni intermediario o soggetto esterno che possa fungere da garante per il loro buon funzionamento. Del resto, gli *smart contract* sono un meccanismo informatico auto-applicativo che garantisce l'esecuzione di un accordo senza la necessità di rimedi giurisdizionali[16]. Questa fiducia incrollabile nel potenziale della *blockchain* ha portato una buona parte dei sostenitori di tali strumenti – e quindi la stragrande parte delle DAO esistenti attualmente – a ritenere superfluo il ricorso a strutture giuridiche che attribuissero un riconoscimento formale all'organizzazione stessa.

Ciò detto, va rilevato come un simile approccio impedisce, in generale, alle DAO di godere dei vantaggi derivanti dall'attribuzione di una forma giuridica societaria di capitali. Nonostante le DAO imitino in una certa misura il funzionamento e la struttura delle società (come i diritti di governance conferiti ai possessori di *token* sulla falsariga delle partecipazioni azionarie), le stesse non beneficiano automaticamente del riconoscimento di una personalità giuridica da parte dell'ordinamento (cui è connesso anche una limitazione della responsabilità).

In generale, quando due o più individui si impegnano in una relazione imprenditoriale anche flebile, possono essere considerati una "società di fatto" (che può essere sottoposta al trattamento delle società di persone – e.g., società in nome collettivo – non iscritte nel registro delle imprese). Tale situazione implica una completa esposizione dei partecipanti (i soci di fatto) ad una responsabilità illimitata ed in solido nei confronti dei creditori dell'organizzazione.

Si potrebbe sostenere che l'esposizione effettiva al rischio di responsabilità illimitata possa essere piuttosto moderata, in quanto DAO progettate in modo adeguato prevedono (*rectius* dovrebbero prevedere) schemi di compensazione specifici e risorse per far fronte automaticamente a ogni possibile rapporto debitorio connesso all'attività realizzata. Esiste, tuttavia, un'ampia gamma di rischi potenziali che difficilmente possono essere previsti *ex ante* in modo efficace che innescano responsabilità risarcitorie da cui i membri della DAO non possono ritenersi esenti. In questo senso gli *smart contract* non necessariamente rappresentano contratti completi, anche negli ambiti teorici di DAO totalmente algoritmiche[17].

Ad esempio, se un tribunale ordinasse ai membri di una DAO non registrata di fornire un risarcimento a favore di un soggetto specifico, le relative risorse finanziarie potrebbero essere rilasciate solo in base al regolamento dell'organizzazione basata sulla *blockchain*. Se l'algoritmo non prevedesse tale soluzione (per le DAO algoritmiche) e se i membri della DAO non fossero disposti a rispettare la sentenza (per le DAO partecipative), la responsabilità potrebbe ricadere congiuntamente su tutti i singoli partecipanti in forza della solidarietà passiva che accomuna i soci della società di fatto.

Questa tipologia di esiti mostra come non sempre è vero che gli *smart contract* vadano ad attuare forme di governance delle transazioni più efficienti rispetto alle gerarchie di impresa e ai contratti relazionali le cui controversie sono risolvibili di fronte a giudici. In alcune circostanze, anzi, essi possono aumentare i costi di transazione, in particolare quando si considera la questione dell'efficienza

15. La materia offre anche ulteriori angoli di indagine, come l'opportunità di estendere il *numerus clausus* agli *smart contract* e alle DAO. Sul punto si rileva come l'approccio più ragionevole alla materia sia di adattarsi alla disciplina giuridica esistente, senza deviare dalla stessa a seconda della tecnologia che viene utilizzata per l'implementazione dei traffici giuridici. Si veda in proposito: Merril–Smith 2000.

16. Davola–Pardolesi 2020; Cuccuru 2017; Raskin 2017.

17. Vatiero 2022.

ex post, ossia dell'adattamento a mutate, imprevedibili ed impreviste circostanze di fatto[18].

Sul punto è opportuno evidenziare come i rimedi giurisdizionali previsti dall'ordinamento possano mal conciliarsi con un sistema tecnologico ingenuamente pensato per essere auto-sufficiente da rimedi esterni. Facendo infatti affidamento su un assunto falso – la presunzione di essere al di fuori dello spazio giuridico – gli sviluppatori di DAO corrono il rischio di elaborare strumenti inadatti ad una efficace gestione imprenditoriale. Allo stesso tempo, un approccio consapevole dei rimedi giurisdizionali che potrebbero incidere sulla vita della DAO potrebbe rendere possibile lo sviluppo di strumenti di governo dell'impresa agevole e migliorativi rispetto a quelli attuali[19].

Non a caso, questo rischio si è concretizzato in diverse pronunce giurisdizionali, in ragione del fatto che le DAO esistenti raccolgono tendenzialmente soggetti che condividono un comune ottimismo nei confronti del potenziale delle applicazioni *blockchain* e sono generalmente consapevoli del rischio di perdere il loro investimento iniziale. Peraltro, per diminuire tali disincentivi, una parte del patrimonio di una DAO potrebbe essere specificamente destinata *ex ante* a funzionare come fondo di autoassicurazione per far fronte a circostanze impreviste che generano obblighi risarcitori[20]. Tuttavia, se e quando le DAO espandono le proprie interazioni di fuori della cerchia ristretta della "comunità dei partecipanti" a mercati di cripto-attività, è altamente improbabile che possano *ex ante* allocare fondi di riserva autoassicurativi sufficienti per coprire tutte i potenziali rischi di passività.

In un regime di responsabilità illimitata, derivante dal mancato uso di forme societarie di capitali con una chiara allocazione di responsabilità, i membri della DAO sono responsabili in solido per il pagamento degli obblighi risarcitori per attività connesse alle attività imprenditoriali realizzate dalla società di fatto. Non sorprende, quindi, che i partecipanti che godono di maggiore liquidità (o percepiti come tali) sarebbero naturalmente i bersagli preferiti dei creditori. Tale contesto è destinato a scoraggiare le persone fisiche e giuridiche con un patrimonio significativo a disposizione (investitori istituzionali e istituzioni finanziarie) dall'aderire o comunque sostenere DAO, creando una selezione finanziaria avversa fra i partecipanti.

3.2. Rappresentanza

La rappresentanza di una organizzazione è il rapporto in base a cui un mandante – l'organizzazione societaria – conferisce poteri di procura ad un soggetto affinché lo stesso (il rappresentante) possa vincolare l'organizzazione verso i terzi. Secondo i principi classici del diritto societario, attraverso il potere di rappresentanza l'amministratore è in grado di manifestare verso i terzi la volontà dell'ente con personalità giuridica, che conseguentemente ne risulta impegnato[21].

Nelle società di persone, prive di personalità giuridica autonoma rispetto ai soci, la gestione può essere delegata o rimanere in capo ai soci. Individuare chi è il mandatario dell'organizzazione è fondamentale, poiché l'agente dà concretezza alla vita imprenditoriale dell'organizzazione, stipulando contratti, acquistando proprietà, citando in giudizio, venendo citato in giudizio e così via.

Dal potere di rappresentanza discendono significative responsabilità nei confronti dei terzi e dell'organizzazione stessa. Infatti, nelle società di fatto, il rappresentante (di fatto) è responsabile in solido con il patrimonio sociale e illimitatamente per le obbligazioni che assume. Tuttavia, lo status societario metterebbe al riparo non solo gli azionisti, ma anche il *management* dagli aspetti negativi delle attività aziendali. Inoltre, la responsabilità degli amministratori è ulteriormente limitata dal rischio di azioni risarcitorie in forza della c.d. *business judgement rule*[22]: regola sviluppatasi nei paesi di *common law*, ma che viene

18. Vatiero 2024.

19. Borgogno–Martino 2024.

20. *United States District Court in Sarcuni v bZx DAO*, No 22-cv-0618 (S.D. Cal. 27 marzo 2023).

21. Armour–Eidenmüller 2020.

22. La *Business Judgment Rule* è un principio giuridico di origine anglosassone, adottato nel diritto societario di vari ordinamenti, che mira a proteggere gli amministratori di una società da responsabilità per le decisioni

applicata costantemente anche dalla giurisprudenza italiana[23].

Per le DAO, si pongono quindi due questioni fondamentali: chi può agire in nome e per conto dell'organizzazione? Quale regime di responsabilità si applica a tale soggetto?

In linea di principio, tecnicamente le DAO non possono avere un apparato organizzativo che vada oltre a quanto previsto dal codice sottostante. Tuttavia, il sistema giuridico richiede che le azioni siano attribuibili a una persona fisica o giuridica. Il problema dell'attribuzione di poteri di rappresentanza è radicalmente diverso nel caso di operazioni completamente interne alla *blockchain* rispetto a quando la DAO interagisce con soggetti al di fuori dell'ecosistema DLT. Nel primo caso, il problema della rappresentanza è residuale e coincide in larga misura con il problema della responsabilità illimitata dei membri in caso di liquidazione giudiziale. Nel secondo caso, il problema è cruciale anche per l'effettiva capacità dell'organizzazione di interagire con attori esterni, che è cruciale per rendere effettivamente possibile l'impiego delle DAO nell'economia reale.

In termini di regime di responsabilità, in assenza di esplicite disposizioni di legge, è improbabile che la responsabilità limitata nonché gli obblighi di diligenza nell'esecuzione dei compiti gestori possano essere applicati al soggetto che agisce, senza alcuna procura formale, in nome della DAO. La responsabilità illimitata, peraltro, sembra conseguenza della inesistenza di una società di capitali e della eventuale configurabilità di una società di fatto, in un ambito di "rappresentanza di fatto". Pertanto, coloro che agiscono a nome delle DAO sarebbero responsabili dell'intero complesso degli obblighi che fanno capo alla DAO stessa.

L'individuazione del soggetto che può essere considerato un rappresentante ("di fatto") di una DAO è un compito complesso e il relativo dibattito rispecchia in gran parte quello sulla responsabilità illimitata dei suoi membri.

In generale, è probabile che, nella prassi, i partecipanti che detengono la maggioranza dei *token* agiscano al pari di rappresentanti di fatto. Tuttavia, parte della dottrina anglosassone sostiene che anche gli sviluppatori del protocollo dovrebbero essere considerati rappresentanti e tenuti a rispettare doveri fiduciari nei confronti degli altri detentori di *token*[24]. L'incertezza su questo punto resta tuttavia molto marcata.

3.3. *Corporate governance*

Sfruttando gli *smart contract* basati sulla *blockchain*, le DAO offrono la possibilità di semplificare gli schemi di voto e di coinvolgere un maggior numero di partecipanti nella governance e nel processo decisionale. In definitiva, in linea con il mantra della comunità dei sostenitori della DLT, ciò consentirebbe la decentralizzazione e disintermediazione della governance imprenditoriale. Poiché un maggior numero di decisioni gestorie potrebbe essere preso dai detentori di *token*, si è ipotizzato che le DAO possano fare a meno di amministratori per gestire l'organizzazione.

Nonostante l'entusiasmo per la governance decentralizzata e la semplicità del processo decisionale propugnato dagli sviluppatori delle DAO, questi elementi non sembrano al momento sufficienti per rendere completamente superflui i tradizionali sistemi di governo dell'impresa. Del pari, l'implicita assunzione in base a cui la completa trasparenza e il decentramento decisionale in un'organizzazione imprenditoriale siano sempre utili e desiderabili è difficilmente compatibile con un quadro ottimale di incentivi capace di garantire il funzionamento della DAO stessa[25].

In effetti, il voto diretto implica una costante attività ed aggiornamento informativo da parte dei detentori di *token*. Nell'ambito delle DAO partecipative ad ampia diffusione, è tuttavia improbabile che un'ampia schiera di detentori di *token* abbia il

gestionali errate, purché queste decisioni siano state prese in buona fede, senza conflitti di interesse e con la dovuta diligenza. Badawi 2023; Benedetti 2019; Piscitello 2012.

23. *Inter alia*: Cassazione Civile, Sezione I, 26 giugno 2001, n. 8621, in cui si riconosce che la responsabilità degli amministratori non può essere automaticamente desunta dal risultato sfavorevole di una decisione gestionale. La Corte ha stabilito che la valutazione deve concentrarsi sulla diligenza e sulla correttezza del processo decisionale.

24. Haque–Seira–Plummer–Rosario 2019; Walch 2019.

25. Schuster 2021; Walker 2021.

tempo e le competenze per impegnarsi in modo significativo nelle quotidiane scelte di gestione dell'organizzazione, il che può portare, di fatto, ad una governance centralizzata nelle mani di pochi grandi detentori di *token* ("balene") soprattutto in caso di voto ponderato sui *token*. In effetti, i concetti di "democrazia diretta" e di partecipazione attiva dei membri applicati alle DAO hanno mostrato tutti i loro limiti con riferimento al tradizionale problema societario dell'apatia degli azionisti di minoranza[26]. La persistenza di tale fenomeno comporta dunque l'emersione con riguardo alle DAO delle stesse problematiche di azzardo morale affrontate dalla *corporate governance* classica, come l'abuso decisionale dei soci di maggioranza a discapito di quelli di minoranza, dimostrando una volta ancora come le DAO siano destinate ad avvalersi dei meccanismi giuridici esistenti piuttosto che a sostituirli in modo drastico.

Allo stesso tempo, in una DAO caratterizzata da alta partecipazione dei detentori di *token*, si può assistere ad un "sovraccarico propositivo"[27], che può essere difficile da gestire, portando a paralisi e/o a fenomeni di "competizione per la selezione dell'attenzione", dove il possibile contrasto tra le volontà dei membri ben potrebbe generare maggiori inefficienze rispetto alle organizzazioni gerarchiche tradizionali.

Per risolvere questi problemi, sono stati proposti nuovi approcci per facilitare la partecipazione alle decisioni relative alla governance e aumentare il coinvolgimento dei partecipanti. Per esempio, vi sono DAO in cui i voti sono ponderati in base a quanto tempo un possessore di *token* sostiene una specifica proposta, per tenere conto della convinzione e del "peso" delle preferenze nelle proprie posizioni dei singoli partecipanti. Un altro meccanismo alternativo è il cosiddetto "voto quadratico"[28], in cui si abbandona un sistema lineare di aggregazione dei voti, considerandone invece la radice quadrata[29]. Infine, gli sviluppatori hanno cercato di affrontare il problema replicando alcuni meccanismi tradizionali del diritto societario, come il voto per delega e il quorum[30]. Se da un lato tali meccanismi mirano a garantire un livello basilare di coordinamento e funzionamento dell'organizzazione, dall'altro va rilevato come gli stessi finiscano inevitabilmente per contraddire i principi di decentralizzazione e democrazia diretta propugnata dagli ideatori delle DAO, evidenziando probabilmente insanabili conflittualità endogene a tali modelli (*trade-off*).

Un modo più drastico per aggirare le problematiche legate alla razionalità limitata degli individui e alle asimmetrie informative è quello, sopra menzionato, di affidarsi a DAO altamente

26. Ding–Xu–Wang–Lee 2023; Allen–Berg–Lane–Potts 2020.

27. Oltre a votare, i detentori di *token* possono avere il diritto di proporre nuove iniziative o cambiamenti all'interno della DAO. Proprio per ridurre il rischio di "sovraccarico propositivo", la capacità di proporre decisioni importanti è solitamente riservata a chi possiede una quantità significativa di *token*.

28. Dimitri 2022.

29. Il costo di acquisto del potere di voto è quindi convesso: è stato dimostrato che questo meccanismo alternativo di ponderazione ripristina l'ottimalità quando gli elettori possono valutare perfettamente la qualità delle proposte che stanno votando, cfr. Lalley–Weyl 2018.

30. In generale, nel contesto della *blockchain* e della governance decentralizzata, il quorum rappresenta il numero minimo di partecipanti (o nodi, o voti) necessari affinché una decisione possa essere considerata valida o esecutiva. Esistono vari modi per definire il quorum in una *blockchain*, a seconda delle esigenze della rete, e.g., (i) quorum basato sul numero di partecipanti, dove si richiede che un certo numero o percentuale di nodi o validatori partecipi al processo per considerare valida una decisione; (ii) quorum basato sullo *stake*: in un sistema "*proof-of-stake*" (protocollo basato sul principio che a ogni utente venga richiesto di dimostrare il possesso di un certo ammontare di criptovaluta), il quorum può essere determinato in base alla quantità di criptovaluta posseduta; (iii) quorum ponderato sui *token* di governance, specialmente nelle DAO, il quorum può essere stabilito in base alla percentuale di *token* di governance utilizzati per votare su una proposta; (iv) quorum dinamico, implementato da alcuni sistemi in cui il numero minimo richiesto può variare in base a determinati fattori, come il livello di attività della rete o la natura della proposta.

algoritmiche[31]. Tale opzione implica che i possessori di *token* debbano fidarsi completamente del buon funzionamento dell'algoritmo sottostante che guida le decisioni gestorie. In tale contesto, l'unico strumento di governance dei partecipanti all'organizzazione è quello della scelta di acquistare – o meno – i relativi *token*. Una simile tipologia di DAO si fonda sul presupposto (tuttora in gran parte, se non del tutto, astratto) che il codice sottostante sia effettivamente capace di perseguire in autonomia l'oggetto sociale nonché di assumere decisioni gestorie, anche di carattere straordinario, in modo continuo. In particolare, tale concetto implica la capacità di affidarsi a sistemi di intelligenza artificiale per gestire automaticamente un'organizzazione complessa, rendendo in ultima analisi possibile la creazione di organizzazioni imprenditoriali a c.d. "guida autonoma"[32].

Infine, in caso di malfunzionamento o "bug" nel software o di problemi dovuti a circostanze impreviste che causano interruzioni tecniche alla DAO, i membri possono abbandonarla o modificare il software sottostante, dando luogo a una revisione radicale della DAO con regole aggiornate, sperando che gli altri detentori di *token* accettino di restare nella nuova organizzazione (c.d. rischi di *fork*)[33]. D'altra parte, come accennato, gli aggiornamenti critici al protocollo (inclusi i cosiddetti *hard fork*) possono richiedere un "consenso qualificato della comunità", attraverso quorum di numero minimo di nodi o partecipanti alla rete che devono accettare il cambiamento per renderlo effettivo. Può quindi essere difficile apportare modifiche significative ai suoi protocolli o ai suoi *smart contract* senza il consenso di una maggioranza significativa e questo può rendere difficile rispondere a problemi tecnici o situazioni di emergenza che richiedono interventi rapidi.

Per eliminare disincentivi *ex ante* alla partecipazione, un numero crescente di DAO avviate di recente fornisce ai membri meccanismi di ritiro dell'investimento iniziale in qualsiasi momento, in modo da assicurare la massima liquidità all'investimento effettuato. Questo processo, chiamato enfaticamente "*rage quitting*", fornisce ai membri un'opzione di ripensamento e un certo grado di controllo su tutti i fondi depositati in una DAO. In sintesi, i membri possono votare per impiegare le risorse per uno scopo specifico o possono ritirare il loro capitale se non sono d'accordo con le scelte assunte dall'organizzazione.

3.4. *Token* di partecipazione

La maggior parte delle DAO si avvale di *token* che forniscono diritti tradizionalmente ricompresi negli schemi commercialistici (ad esempio, un *token* digitale che fornisce esclusivamente la possibilità di influire su alcune decisioni gestorie); è molto discusso se possano essere considerati al pari di azioni e quote di società di capitali.

Peraltro, oltre a (i) funzione di "governance", in alcune DAO i *token* hanno anche (ii) funzioni di "utilità" e (iii) funzioni di "ricompensa" e (iv) funzioni "puramente finanziarie". Per quanto concerne i *token* di "utilità", alcune DAO emettono *token* che, se acquistati, danno accesso a servizi o prodotti all'interno dell'ecosistema della DAO. Per quanto concerne, invece, i *token* di "ricompensa", molte DAO utilizzano *token* per premiare i membri per il loro contributo all'ecosistema (ad esempio, per aver fornito liquidità a un protocollo DeFi, sviluppato nuove funzioni o partecipato attivamente alla community). Questi *token* possono avere valore di mercato e possono essere scambiati o utilizzati all'interno della DAO stessa. Infine, *token* "puramente finanziari" sono assimilabili a diritti

31. Molte DAO algoritmiche sono utilizzate nel contesto della finanza decentralizzata (DeFi) e delle "*stablecoin*", dove gli algoritmi gestiscono automaticamente l'emissione, il ritiro o la regolazione dei *token* per mantenere stabilità o efficienza in un sistema economico decentralizzato. Le "*stablecoin*" sono criptovalute il cui valore è ancorato, o legato, a quello di un'altra valuta, merce o strumento finanziario, che mirano a fornire un'alternativa all'elevata volatilità delle criptovalute più popolari, tra cui il Bitcoin (BTC). In questi sistemi, algoritmi governano l'offerta monetaria, cercando di mantenere il valore stabile, senza l'intervento di una governance manuale. Esempi includono: Ampleforth (AMPL), ed anche Terra (LUNA/UST).

32. Cfr. Abriani–Costi 2023; Armour–Eidenmüller 2020.

33. Come nelle *blockchain*, che ne sta alla base, anche nelle DAO esiste la possibilità di divisioni interne tra i partecipanti, che possono portare a *fork* o scissioni. Questo si verifica quando una parte della comunità non è d'accordo con le decisioni prese e crea una nuova versione dell'organizzazione con regole o obiettivi diversi.

di dividendo o ad altre forme di reddito, che ben potrebbe essere considerato un strumento finanziario ai sensi della normativa italiana e europea (come la MiFID II).

La variabilità delle funzioni dei *token* e dei modelli esistenti di DAO rende molto complesso una qualificazione generale dei primi così come delle seconde.

I confini tra i *token* di governance e gli strumenti finanziari tradizionali sono molto sfumati. Diritti patrimoniali, diritti amministrativi, diritti di governance e diritti di utilità possono essere associati ai *token*, che vengono poi venduti con modalità simili a quelle di un'offerta pubblica iniziale tradizionale.

Le giurisdizioni di tutto il mondo sono alle prese con la questione se i *token* debbano essere trattati come strumenti finanziari dal punto di vista giuridico. Se lo sono, ne consegue che l'emittente deve rispettare i requisiti e gli obblighi regolamentari applicabili a tali beni.

Peraltro, tali questioni sono destinate a influenzare la capacità dei mercati di attribuire un prezzo affidabile ai *token*. Allo stato attuale, i costi di informazione sono significativi, in quanto gli operatori di mercato dovrebbero comprendere tutte le funzioni associate ai *token*, ed il significato e il funzionamento del codice incorporato in una specifica DAO (anche per i soli *token* di governance).

Anche se un'analisi approfondita della regolazione finanziaria relativa ai *token* esula dallo scopo del presente lavoro, vale la pena sottolineare che l'ordinamento privato da solo potrebbe non garantire l'efficienza informativa dei mercati delle criptovalute e dei cripto-asset. Pertanto, poiché i *token* sono un elemento cruciale nel funzionamento delle DAO, ogni nuova iniziativa legislativa sul punto dovrebbero mirare a chiarire la qualificazione giuridica di questi nuovi asset.

4. L'evoluzione della disciplina giuridica delle DAO in Ue e USA

Uno dei fondamentali problemi giuridico-economici delle DAO, come visto, è inerente al loro inquadramento sotto un profilo giuridico, ossia a questioni ed incertezze inerenti alla mancanza di una personalità giuridica chiara o un'identità legale riconosciuta dagli ordinamenti giuridici esistenti.

Per questi motivi, un numero piccolo ma crescente di DAO è stato registrato, costituendosi come società di capitali in conformità a selezionate e favorevoli giurisdizioni, ottenendovi personalità giuridica. Un numero crescente di DAO ha infatti ottenuto personalità giuridica costituendosi in giurisdizioni con un quadro fiscale e giuridico favorevole (ad esempio, le Isole Cayman, Singapore, Panama, Svizzera e Irlanda). Queste giurisdizioni hanno offerto l'opportunità di creare fondazioni con una struttura di governance molto flessibile. Tale struttura giuridica garantisce che le proposte implementate sulla *blockchain* possano essere riflesse dagli organi decisori della fondazione. Tuttavia, il ricorso ad una giurisdizione estera rispetto al centro di interesse della DAO comporta notevoli barriere all'ingresso per i partecipanti e nuovi non triviali problemi di incertezza giuridica (giurisdizione), in particolare, dal punto di vista del diritto fiscale e del diritto del lavoro applicabile.

Come visto nelle precedenti sezioni, il ricorso a forme societarie di capitali presenta una serie di elementi di indubbia utilità che potrebbero rivelarsi positivi anche per il migliore funzionamento delle DAO. Da un lato, tuttavia, tale rilievo è in contrasto con le rappresentazioni più pure del modello organizzativo autonomo e decentrato, secondo cui le implementazioni legate alla *blockchain* sarebbero state destinate a rendere non necessari i sistemi giuridici nazionali. Dall'altro lato, le prime iniziative giuridiche specifiche esistenti tendono verso un certo grado di "ibridazione" del modello DAO, introiettando elementi delle strutture societarie riconosciute nei vari ordinamenti. Tale processo normativo di "ibridazione" sembra cercare un bilanciamento fra i trade-off endogeni esistenti, ossia il legislatore deve definire il perimetro entro cui la governance basata sulla *blockchain* possa essere giuridicamente equiparata a meccanismi societari tradizionali, senza tuttavia forzare gli sviluppatori DAO a replicare su *blockchain* modelli di funzionamento tradizionali, disperdendo il potenziale innovativo della DLT stessa[34].

Le nuove iniziative legislative in materia di DAO si concentrano infatti sul loro status giuridico e sul regime giuridico applicabile ai *token*. Non viene invece affrontata la questione della governance decentralizzata.

34. Borgogno–Martino 2024.

Sebbene l'Ue non abbia ancora definito un approccio legislativo specifico per le DAO, nel settembre 2020 la Commissione europea ha presentato una proposta di regolamento sui mercati dei cripto-asset (MiCA) per stabilire una cornice giuridica uniforme di disciplina delle cripto-attività[35]. Questo atto legislativo ha lo scopo di stabilire regole uniformi in materia di trasparenza e requisiti informativi per l'emissione, l'offerta al pubblico e l'ammissione alla negoziazione di cripto-attività. Inoltre, sono previste norme sull'autorizzazione e la vigilanza dei fornitori di servizi di cripto-attività e dei loro emittenti.

Il Regolamento è entrato in vigore nel giugno 2023 per diventare pienamente applicabile a partire dal 30 dicembre 2024. È tuttavia utile evidenziare come la Commissione per gli affari economici e monetari del Parlamento europeo, nell'ambito del trilogo, avesse proposto di modificare la bozza originaria con specifiche disposizioni riguardanti le DAO[36]. Secondo il Parlamento europeo, un nuovo considerando avrebbe infatti dovuto riconoscere che alcuni tipi di cripto-attività non sono emesse da soggetti registrati, ma sono invece gestite da organizzazioni autonome decentralizzate.

In particolare, la bozza conteneva una definizione di DAO, intesa come "un sistema organizzativo basato su regole che non è controllato da alcuna autorità centrale e le cui regole sono interamente contenute nel suo algoritmo"[37]. Secondo tale proposta, le DAO sarebbero dunque dovute essere autorizzate ad offrire cripto-attività al pubblico o a chiedere l'ammissione di tali cripto-attività alla negoziazione su una piattaforma apposita. Detto questo, il Parlamento europeo ha proposto di affidare alle autorità competenti il compito di garantire che le DAO rispettino tutti i requisiti previsti dal Regolamento (come la notifica e la pubblicazione di un apposito libro bianco e il regime di autorizzazione)[38].

Nonostante la proposta del Parlamento, la versione finale del Regolamento MiCA non menziona esplicitamente le DAO. Ciò significa che le DAO completamente decentralizzate non sono ricomprese nell'ambito oggettivo del MiCA. Tuttavia, le azioni dei singoli partecipanti alle DAO possono essere ricomprese nel perimetro del Regolamento. Quando infatti una DAO, anche se non completamente decentralizzata, emette *token* classificati come cripto-attività e fornisce servizi che rientrano nell'ambito di applicazione del MiCA, deve rispettare i requisiti posti dal regolamento stesso.

A partire dall'entrata in vigore del MiCA, al termine del 2024, le DAO devono quindi munirsi di specifica personalità giuridica in modo da garantire un livello minimo di protezione degli interessi dei terzi. Devono inoltre essere soggette a una vigilanza prudenziale adeguata alla loro forma giuridica. Ad esempio, le DAO potrebbero emettere cripto-attività, ma queste potranno essere offerte ai cittadini europei solo da una *Crypto Asset Service Provider* (CASP) registrata. In particolare, il MiCA non specifica la particolare forma di personalità giuridica che le DAO dovrebbero adottare, il che potrebbe portare a una possibile frammentazione normativa[39].

Con riferimento agli Stati Uniti, va invece rilevato come né il Congresso né alcuna agenzia federale abbiano approvato regolamenti specifici sulle DAO. Tuttavia, il 7 giugno 2022, la senatrice Kirsten Gillibrand (D-NY) e la senatrice Cynthia Lummis (R-WY) hanno introdotto il *Responsible Financial Innovation Act* (RFIA) con l'obiettivo di stabilire un quadro normativo completo per gli asset digitali negli Stati Uniti[40]. Nel luglio 2023 la proposta è stata emendata per incorporare i suggerimenti

35. Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.
36. Parlamento europeo, "Report on the proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937", COM(2020) 593, 24 September 2020, C9-0306/2020 – 2020/0265 (COD).
37. *Ivi*, art. 3(1)(1a).
38. *Ivi*, art. 3(b).
39. Naudts 2023.
40. La proposta definisce le DAO come organizzazioni che (i) utilizzano *smart contracts* per il perseguimento di finalità economiche, commerciali, caritatevoli o similari (ii) il cui governo sia implementato in modo diffuso e

ricevuti in fase di consultazione pubblica, tra cui quelli di agenzie di regolamentazione come la *Securities and Exchange Commission* (SEC) e la *Commodities Futures Trading Commission* (CFTC), focalizzati su anti-riciclaggio e regolamentazione finanziaria[41].

Al contempo, siccome la SEC e la CFTC non detengono poteri appositi in materia, hanno attuato una interpretazione estensiva delle norme esistenti, attuando una cosiddetta "regulation by enforcement"[42] con l'obiettivo di definire il quadro giuridico degli asset fondati su *blockchain* applicando il diritto esistente alle cripto-attività innovative.

Come reazione all'inerzia legislativa federale, diversi Stati hanno cercato di colmare il vuoto normativo con iniziative regolamentari su misura per le criptoattività. Il Delaware e il Vermont hanno avviato il dibattito nei propri organi parlamentari, mentre il Wyoming si è affermato come la giurisdizione più accomodante nei confronti delle attività imprenditoriali e organizzative basate su DLT, approvando nel 2021 una legge che permette alle DAO di acquisire lo status di società a responsabilità limitata[43]. Tuttavia, questa iniziativa è stata criticata in quanto eccessivamente manichea: tale legge prevede infatti che tutte le DAO siano implicitamente ricondotte a forme di gestione diretta da parte dei membri, a meno che non scelgano di essere "gestite algoritmicamente"[44]. Ciò significa che una DAO in fase di avvio non può essere alimentata e sviluppata agevolmente da un gruppo iniziale di fondatori, in particolare quando si trova nelle fasi di sviluppo più vulnerabili. Infatti, le DAO vengono spesso avviate in modo centralizzato, riconoscendo una quantità sufficiente di *token* di governance ai fondatori in modo da garantire loro la possibilità di controllarne la gestione ed eventuali future revisioni del codice. Dopo questa fase iniziale, i *token* di governance vengono distribuiti tra gli altri sostenitori (non sviluppatori) come previsto dal protocollo.

Nonostante i problemi attuativi, come detto, questa soluzione riflette il tentativo conciliare le caratteristiche intrinseche delle DAO con le strutture giuridiche societarie esistenti. Tuttavia, le entità giuridiche tradizionali sono state progettate pensando alle società tradizionali e basandosi sulle capacità degli individui del XX secolo di coordinarsi nell'ambito di schemi organizzativi ampi e spazialmente dispersi. È improbabile che il potenziale innovativo delle DAO possa essere sfruttato appieno affidandosi a strutture giuridiche tradizionali che non tengono conto delle caratteristiche intrinseche delle entità basate sulla *blockchain*.

5. Breve conclusione

In via di prima approssimazione, va riconosciuto come gli argomenti usati per giustificare il ricorso alle DAO nella prassi imprenditoriale presentano semplificazioni eccessive. Da un lato, le promesse dei sostenitori delle DAO associano in modo troppo semplicistico l'eliminazione di problemi di governance alla decentralizzazione decisionale. Dall'altro lato, l'autonomia dal sistema giuridico di cui le DAO dovrebbero godere molto spesso non trova conforto nell'odierno contesto giuridico-economico, ma è probabile che si traduca in ulteriori limitazioni e costi associati all'uso delle DAO. Ciò detto, l'affermazione secondo cui le DAO sono sostanzialmente inutili al di fuori dei limitati casi riguardanti comunità chiuse di utilizzatori di

distribuito tra i titolari di *token*, e che (iii) sono costituite secondo il diritto nazionale rilevante come una organizzazione autonoma e decentralizzata, cooperativa, fondazione, o altre simili entità. Cfr: *Lummis, Gillibrand Introduce Landmark Legislation To Create Regulatory Framework For Digital Assets*, Press Release 2022.

41. *Lummis, Gillibrand Reintroduce Comprehensive Legislation To Create Regulatory Framework For Crypto Assets*, Press Release 2023.
42. Con il termine *regulation-by-enforcement* (regolazione tramite l'applicazione) si intende l'approccio adottato dalle agenzie federali statunitensi in base a cui il diritto esistente viene applicato in modo da ricomprendere nel proprio ambito di azione e disciplinare anche fattispecie nuove, non esplicitamente disciplinate dal quadro esistente. Brummer–Yadav–Zaring 2024.
43. Ai sensi del par. 17-31-104(a), una DAO è una *limited liability company* il cui statuto dichiara esplicitamente di avvalersi della DLT per la propria organizzazione.
44. Il testo legislativo non definisce cosa si intenda per organizzazione "gestita algoritmicamente".

cripto attività non tiene conto del potenziale tecnologico che la *blockchain* e le DAO stesse possono offrire rispetto alla teoria dell'impresa e dell'organizzazione commerciale.

Questo articolo vuole offrire prime riflessioni di inquadramento giuridico-economico delle DAO prestando attenzione alla cornice di incentivi definita dall'analisi economica del diritto, cercando quindi di porre alcune basi di analisi di impatto per un possibile futuro inquadramento normativo delle DAO come specifiche organizzazioni imprenditoriali.

A questo riguardo, sotto un profilo di analisi economica del diritto, è fondamentale comprendere l'effettiva capacità delle soluzioni algoritmiche di risolvere i problemi di agenzia, opportunismo contrattuale e costi di transazione che contraddistinguono le organizzazioni imprenditoriali. Pur non potendo offrire una risposta univoca, è possibile affermare che le DAO hanno il potenziale di dimostrarsi migliorative non in via generale, ma soltanto con riferimento a casi d'uso specifici interni all'ecosistema *blockchain*.

Infine, l'analisi porta in luce i tratti innovativi delle DAO, intese come strumenti al servizio dell'organizzazione imprenditoriale. Tali strutture appaiono infatti utili ogniqualvolta sia necessario raggiungere un'elevata automazione del funzionamento societario, come la segmentazione del patrimonio sociale e la trasferibilità dei *token*. D'altra parte, per tutti gli aspetti caratterizzati da una chiara allocazione di responsabilità in capo ad una o più persone fisiche, come la responsabilità dei membri e la rappresentanza, allo stato giuridico attuale, le DAO si dimostrano inadatte per interagire utilmente con soggetti esterni all'ecosistema *blockchain*.

Con riferimento all'analisi giuridica, sembra opportuno privilegiare l'adozione di una regolazione specifica delle DAO. Allo stesso tempo, è evidente come le iniziative legislative finalizzate finora tra Unione europea e Stati Uniti non sembrano prendere in adeguata specifica considerazione le caratteristiche tecnologiche delle DAO, creando potenzialmente una inefficiente frammentazione ed incertezza normativa.

A questo riguardo, un'alternativa interessante ma non meno problematica sotto un profilo attuativo, rispetto alla creazione di nuove forme di DAO ibride è la proposta di dare risalto e seguire un principio di "equivalenza normativa"[45]. Questo concetto richiederebbe l'identificazione degli obiettivi di policy o, in altri termini, dell'interesse pubblico sottostante alle rilevanti normative esistenti, al fine di comprendere se la tecnologia DTL sottostante ad una specifica DAO (o sue specifiche configurazioni) possa raggiungere lo stesso obiettivo di interesse pubblico, essendo così di fatto soggetta alle stesse regole già previste per le imprese tradizionali.

Tale approccio consisterebbe quindi nella definizione normativa di principi generali di equivalenza, la cui attuazione andrebbe delegata all'attività *ex post* di verifica da parte di autorità amministrative o giurisdizionali (che garantiscano una uniformità applicativa almeno a livello continentale).

Un esempio significativo di equivalenza normativa è la relazione tra i requisiti di registrazione per le persone giuridiche e l'impiego di una DAO su DLT. Gli obblighi di registrazione sono giustificati dall'obiettivo di garantire un'ampia pubblicità e affidabilità delle operazioni giuridiche riguardanti l'organizzazione cui è concessa personalità giuridica dall'ordinamento. A tali fini, appositi soggetti pubblici sono incaricati di verificare la veridicità del processo e la corretta diffusione delle informazioni relative all'organizzazione. Allo stesso modo, l'implementazione di uno *smart contract* su una *blockchain* con dati rilevanti su una DAO potrebbe raggiungere gli obiettivi di pubblicità e certezza con strumenti diversi.

Questo approccio potrebbe rappresentare una alternativa all'attuale tendenza alla frammentazione che caratterizza diversi sistemi di *corporate governance*. Inoltre, l'equivalenza normativa permetterebbe di integrare nuove tecnologie nel quadro giuridico esistente, non richiedendo riforme giuridiche su larga scala. L'avvio di esperimenti regolamentari tramite *sandbox* potrebbe rivelarsi utile per testare tali nuove soluzioni e valutare la loro capacità di adeguarsi con gli obiettivi di politica del diritto perseguiti dagli ordinamenti nazionali.

45. La proposta è stata avanzata nel novembre del 2021 dalla Coalition of Automated Legal Applications (COALA), *Model Law for Decentralized Autonomous Organizations*, 2021.

Riferimenti bibliografici

N. Abriani, R. Costi (a cura di) (2023), *Diritto societario, digitalizzazione e intelligenza artificiale*, Giuffrè, 2023

J.G. Allen (2020), *Bodies without Organs: Law, Economics, and Decentralised Governance*, in "Stanford Journal of Blockchain Law & Policy", vol. 4, 2020, n. 1

D.W.E. Allen, C. Berg, A.M. Lane, J. Potts (2020), *Cryptodemocracy and its institutional possibilities*, in "The Review of Austrian Economics", vol. 33, 2020, n. 3

F. Annunziata, A.C. Chisari, P.R. Amendola (2023), *DLT-Based Trading Venues and EU Capital Markets Legislation: State of the Art and Perspectives Under the DLT Pilot Regime*, in "The Italian Law Journal", vol. 9, 2023, n. 1

J. Armour, H. Eidenmüller (2020), *Self-Driving Corporations?*, in "Harvard Business Law Review", vol. 10, 2020, n. 1

A.B. Badawi (2023), *The Business Judgment Rule*, in Id. (ed.), "Corporate Law and Economics - Encyclopedia of Law & Economics", vol. 2, Edward Elgar, 2023

L. Benedetti (2019), *L'applicabilità della* business judgment rule *alle decisioni organizzative degli amministratori*, in "Rivista delle società", 2019, n. 2-3

O. Borgogno (2018), *Smart contracts as the (New) Power of the Powerless? The Stakes for Consumers*, in "European Review of Private Law", vol. 26, 2018, n. 6

O. Borgogno, E.D. Martino (2024), *Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype*, in "Law, Innovation and Technology", vol. 16, 2024, n. 2

C. Brummer, Y. Yadav, D.T. Zaring (2024), *Regulation by Enforcement*, in "University of Southern California Law Review", vol. 96, 2024, n. 6

I. Capelli (2023), *La struttura finanziaria delle imprese e gli strumenti finanziari digitali. Prime considerazioni tra decentralizzazione e regolazione nel contesto del DLT Pilot Regime e del Decreto FinTech*, in "Il diritto dell'informazione e dell'informatica", 2023, n. 4-5

P. Carrière (2023), *Decreto Fintech e MICAR: il quadro normativo sulle cripto-attività*, in "DB non solo diritto bancario", 30 maggio 2023

P. Carrière, N. de Luca, M. de Mari et al. (2023), *Tokenizzazione di azioni e azioni tokens*, in "Quaderni giuridici Consob", n. 25, gennaio 2023

V.V. Cuocci, F.P. Lops, C. Motti (a cura di) (2021), *La circolazione della ricchezza nell'era digitale*, Pacini Giuridica, 2021

P. Cuccuru (2017), *Beyond Bitcoin: An Early Overview on Smart contracts*, in "International Journal of Law and Information Technology", vol. 25, 2017, n. 3

A. Davola, R. Pardolesi (2020), *What Is Wrong in the Debate about Smart contracts*, in "Journal of European Consumer and Market Law", vol. 9, 2020, n. 5

N. Dimitri (2022), *Quadratic Voting in Blockchain Governance*, in "Information", vol. 13, 2022, n. 6

Q. Ding, W. Xu, Z. Wang, D.K.C. Lee (2023), *Voting Schemes in DAO Governance*, in "World Scientific Annual Review of Fintech", vol. 1, 2023

M. Doria, F. Bassan, M. Rabitti et al. (2024), *Caratteristiche degli smart contracts*, in "Questioni di Economia e Finanza", Occasional Papers, 2024, n. 863

Q. DuPont (2017), *Experiments in Algorithmic Governance. A History and Ethnography of "The DAO, a Failed Decentralised Autonomous Organization*, in M. Campbell-Verduyn (ed.), "Bitcoin and beyond", Routledge, 2017

C. Gola, V. Cappa, P. Fiorenza et al. (2023), *La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti*, in "Questioni di Economia e Finanza", Occasional Papers, 2023, n. 771

R. Haque, R. Seira, B. Plummer, N. Rosario (2019), *Blockchain Development and Fiduciary Duty*, in "Stanford Journal of Blockchain Law & Policy", vol. 2, 2019, n. 2

S.P. Lalley, E.G. Weyl (2018), *Nash equilibria for quadratic voting*, in "Microeconomics: Welfare Economics & Collective Decision-Making eJournal", 2018

A. Laudonio (2023), Distributed ledger technology *e* ICOs *(una favola giuridica sisifea sul diritto dei mercati finanziari e l'innovazione)*, in "Rivista di diritto bancario", 2023, n. 1

V. Lemma (2023), *DLT pilot: verso il mercato degli strumenti finanziari digitali*, in "DB non solo diritto bancario", 2 maggio 2023

E.D. Martino, W.-G. Ringe (2024), *The Social Cost of Blockchain. Externalities, Allocation of Property Rights, and the Role of the Law*, in "ILE Working Paper Series", 2024, n. 80

T.W. Merril, H.E. Smith (2000), *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, in "Yale Law Journal", vol. 110, 2000, n. 1

E. Naudts (2023), *The future of DAOs in finance: In need of legal status*, in "ECB Occasional Paper Series", 2023, n. 331

P. Piscitello (2012), *La responsabilità degli amministratori di società di capitali tra discrezionalità del giudice e* business judgement rule, in "Rivista delle Società", 2012, n. 6

R. Piselli (2019), *Quando la decentralizzazione delle DLT incontra il mercato dei capitali. Appunti sulle organizzazioni decentralizzate*, in "Analisi Giuridica dell'Economia", 2019, n. 1

C. Poncibò (2020), *Il Diritto Comparato e la Blockchain*, Edizioni Scientifiche Italiane, 2020

M. Raskin (2017), *The Law and Legality of Smart Contracts*, in "Georgetown Law Technology Review", vol. 1, 2017, n. 2

S. Rigazio (2021), Smart contracts *e tecnologie basate su registri distribuiti nella L. 12/2019*, in "Il diritto dell'informazione e dell'informatica", 2021, n. 2

M.T. Rodi, V. Santoro, (2024), *Prime considerazioni sulle disposizioni urgenti in materia di strumenti finanziari in forma digitale*, in "Diritto della banca e del mercato finanziario", 2024, n. 1

U.R. Rodrigues (2019), *Law and the Blockchain*, in "Iowa Law Review", vol. 104, 2019, n. 2

J. Rohr, A. Wright (2019), *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, in "Hastings Law Journal", vol. 70, 2019, n. 2

E. Schuster (2021), *Cloud Crypto Land*, in "The Modern Law Review", vol. 84, 2021, n. 5

M. Vatiero (2024), *The "dark side" of smart contracts: A contract theory perspective*, in "European Management Review", vol. 21, 2024, n. 3

M. Vatiero (2022), *Smart contracts vs incomplete contracts: A transaction cost economics viewpoint*, in "Computer Law & Security Review", vol. 46, 2022

A. Walch (2019), *In Code (Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, in P. Hacker, I. Lianos, G. Dimitropoulos, S. Eich (eds.), "Regulating Blockchain: Techno-Social and Legal Challenges", Oxford University Press, 2019

M. Walker (2021), '*Unnecessary complexity': the crypto industry's continuing efforts to avoid regulation*, in "LSE Business Review", 2021

A. Wright (2021), *The Rise of Decentralised Autonomous Organizations: Opportunities and Challenges*, in "Stanford Journal of Blockchain Law & Policy", vol. 4, 2021, n. 2

A. Wright, P. De Filippi (2015), *Decentralised Blockchain Technology and the Rise of Lex Cryptographia*, in SSRN, 2015

D. Yermack (2017), *Corporate Governance and Blockchains*, in "Review of Finance", vol. 21, 2017, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0205 • articolo sottoposto a peer review • pubblicato in anteprima il 10 apr. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Fabrizio Corona – Moreno Ferrarese

The future without a Judge

Is it possible to replace the judge's decision with an algorithm? This paper explores the computational evidence regarding the use of Opinion Mining Sentiment Analysis and lexical spinners by computational machines, highlighting the challenges associated with the use of algorithms in a quali-quantitative predictive context. The research focuses on the implementation of an advanced algorithm designed to replace the judge in the judicial activity by adopting an approach that integrates the intensity variables of cognitive stimuli into the parametric analysis through a combination of qualitative and quantitative methods, thus minimising the errors associated with the quantitative-predictive method in isolation. Such an approach allows for the accurate replication of the judge's writing style and decisions, guaranteeing an accurate and unbiased interpretation of legal facts.

Nuncupative language – Entropy and syntropy of language – Algorithm – Lexical machines – AI approach

Il Futuro senza giudice

È possibile sostituire la decisione del Giudice con un algoritmo? Questo articolo esplora l'evidenza computazionale riguardante l'impiego dell'Opinion Mining Sentiment Analysis e degli spinner lessicali da parte di macchine computazionali, evidenziando le sfide associate all'uso di algoritmi in un contesto predittivo quali-quantitativo. La ricerca si concentra sull'implementazione di un algoritmo avanzato, progettato per sostituire il giudice nell'attività giudiziaria adottando un approccio che integra le variabili di intensità degli stimoli cognitivi nell'analisi parametrica attraverso una combinazione di metodi qualitativi e quantitativi minimizzando, così, gli errori legati al solo metodo quantitativo-predittivo. Tale approccio, permette di replicare accuratamente lo stile di scrittura del giudice e le sue decisioni, garantendo un'interpretazione precisa e imparziale dei fatti giuridici.

Linguaggio nuncupativo – Entropia e sintropia del linguaggio – Algoritmo – Macchine lessicali Artificial Intelligence

Fabrizio Corona is post-doc researcher at University of Brescia, adjunct professor in Legal informatics at LUISS Guido Carli and adjunct professor in Legal informatics at Giustino Fortunato University

Moreno Ferrarese is teaching fellow at the Department of Sociology and social research at University of Trento

M. Ferrarese wrote paragraphs 1, 3, 4, 5, 6. F. Corona wrote paragraphs 2, 7, 8, 9. Paragraph 10 results from common considerations

Summary: 1. Strengths and weaknesses of the *inanimate judge*. – 2. The *Noetics* of the judge. – 3. The *legal constraints* for a non-human judge. – 4. Communication *Meta-referents for a Robotic Judgement*. – 5. *Algorithms* for a Robotic Justice. – 6. *Keywords* as headwords for robotic judgments – 7. The *acceptance* of judgments. – 8. The physiological limits of the human judge. – 9. Will there ever be a *just judge*? – 10. Concluding reflections.

"A robot may not injure a human being or, through inaction,
allow a human being to come to harm.
A robot must obey any orders given to it by human beings,
except where such orders would conflict with the First Law.
A robot must protect its own existence as long as such protection
does not conflict with the First or Second Law".

Isaac Asimov, *Handbook of Robotics*, 56th Edition 2058 A.D.

1. Strengths and weaknesses of the *inanimate judge*

The dialectical structure of the proceedings requires that the interested parties addressees of the effects of the *petitum* always participate in the preparatory phase of the measure, and that, in the procedural phase of the trial, powers, faculties and duties relating to the distributive exercise of the rule between the participants in the procedural action are represented, in order to implement an effective correspondence and equivalence between the positions represented.

Therefore, the dialectical development of the Italian trial, as conceived by the codes, coincides with a symmetrical structure of the subjective positions, their mutuality and substantial parity that translates, for each of the participants, into the right to exercise a set of controls, relations and choices and the duty to undergo the controls and relations of others during the procedural eloquence, whether cartular with the new Cartabia trial, or oral with the traditional rite.

For such an extensive formulation of the search for balance, Pierre Bourdieu[1] explained that institutions, as such, tend to develop collective and organised defence mechanisms, which are the result of many individual, independent, yet structurally connected actions that contribute to their own self-preservation.

Cassese defines the shape of the judicial institution as "… a judicial body composed of people who are on average well prepared, but closed in on itself, corporative, which cannot find in its experience the ideas to correct itself and which seems incapable of maturing proposals for better systems and of dialogue with culture, the professions, the political world…"[2].

The autonomy of the judiciary, which constitutes a cornerstone of the rule of law and democracy, has given rise to a series of self-referential mechanisms, feeding an ever-increasing number of privileged conditions, if not constituting lobby. The judiciary in our country has increasingly expanded its sphere of influence, often engaging in

1. Bourdieu 2005, p. 101.
2. Cassese 2022, p. 88.

innovative interpretations of the principle of taxativity of criminal cases. This is due to the belief that the judiciary has been entrusted with a social mandate to oversee ethical conduct. The aforementioned point has been corroborated by Beria di Argentine, who notes that historical circumstances have reinforced this belief at times. We could argue that sometimes the court system can be flawed, leading to the perception that justice is not always served. There may be a variety of factors at play, such as bias, prejudice, and unfair expectations, that can create an atmosphere that is disconnected from true justice. Yet, the institution of free conviction has been used precisely to achieve the opposite effect.

The need to identify "instruments for assessing the professional aptitude of the magistrate" was ruled out because it would have violated the principle of free conviction and, therefore, the autonomy and independence of the judiciary. Free conviction "ended up turning into a grossly potestative principle capable of legitimising the arbitrariness of judges".

The overall picture it gives us of the situation of criminal guarantorism in Italy is certainly not edifying. And in the thirty years that have elapsed since these reflections, judicial decisionism has expanded as a result of increasingly vague facts and interpretative processes that, particularly in the criminal sphere, resort to a nonchalant use of extensive interpretation, continually eluding the prohibition of the taxativity of criminal cases.

The law, as we know, is not scientific for the sake of science: being scientific as a means to an end, it must be judged by the results it achieves, not by the subtleties of its internal structure; it must be assessed by the extent to which it achieves its end not by the beauty of its logical processes or the rigour with which it displays its rules[3]. But as the margins of interpretative autonomy have increased, so has the expansion of judicial power interpenetrated with the constant need to define a deontological framework through which to guarantee that affirmation and protection of rights that is entrusted to the judiciary.

Thus, instead of providing a series of principles, we offer a description of certain sensitivities. These include objectivity, comprehension, logical structure, conventional structure, clear and objective language, appropriate formatting, a formal register, clear structure, balance, precise word choice and grammatical correctness. The recognition of the dreadful and repugnant nature of judicial power; the acknowledgement of the relative and uncertain nature of procedural truth and, as a result, the existence of an inevitable margin of illegitimacy in the execution of jurisdiction; the significance of doubt and the realisation of the constant possibility of factual errors; the readiness to consider opposing opinions and the dispassionate search for truth. The principles of equity and singular case assessment must be upheld, while respecting all parties. The ability to instil confidence in all parties, including defendants, is crucial. Magistrates must maintain confidentiality in their trials and avoid any political influence or accusations thereof[4].

The Italian judiciary has undergone a series of deformations over time. Issues within the judiciary system encompass the politicisation of the courts, a narrow view of their duties, slow trial proceedings, misuse of pre-trial detainment, as well as telephone and environmental surveillance, the influence of particular magistrates, consistent breaches of investigative secrecy, and an overtly powerful public prosecutor's office that is exacerbated by the obedience of the overseeing judge.

In the context of the relationship between democratic balances and the autonomy of judges, the interplay between virtue and politics exposes the inadequacy of an unaccompanied professionalism devoid of moral sensitivity and/or social responsibility guided by free will. This represents an additional vulnerability for human judges, despite the need to disregard convictions, states of mind, and passions that may adversely affect decisions in order to uphold legal ethics. Article 54 of the Constitution states that "citizens entrusted with public functions have a duty to perform them with discipline and honour".

There is no public function more delicate than the exercise of justice. If we were to interpret Article 54 of the Constitution correctly in light of this assumption, we would have to conclude that it is not virtue that justifies function, but function

3. Pound 1908, p. 605.

4. Ferrajoli 2013; Nordio 2022, p. 98.

that produces virtue. Paradoxically, our legal culture has not addressed the question of whether the guardians of virtue' should themselves be virtuous or, at least, what qualities they must possess in order to be entrusted with such a delicate task.

According to Article 37(1)(b) of the Code of Criminal Procedure, the judge is only objectionable if he has conditioned the trial with specific acts that are the result of an undue manifestation of his ideas, but it is irrelevant if, in the course of the proceedings, he has shown prejudice, emotion, irritation or intolerance[5].

The judge should be all the freer in his decision-making processes the more responsible he is to the institution he represents and to society. Independence is not an end in itself but is meant to increase the protection of fundamental rights. The Recommendation No. 12 of 17 November 2010 of the Committee of Ministers of the Council of Europe "On Judges: Independence, Effectiveness, Accountability" seems to fully entrust the Superior Council of the Judiciary with the custody of constitutional balances.

The Recommendation does not discuss the judges' quality, except for a clear reference to merit as a means of selecting and evaluating careers. It emphasizes that the external independence of judges is not a personal prerogative or privilege but is essential for the rule of law and for everyone who seeks and expects impartial justice.

The independence of judges must, therefore, be seen as a guarantee of freedom, respect for human rights and the impartial application of the law. Supplanting the inefficiency of the legislature in the face of rapid economic, social, and technological changes, however, ends up by eliding the horizons of legal certainty and the principle of equality.

The absence of both external and internal boundaries detracts from the fundamental tenets of the judiciary, leading to a potential loss of independence. This risk can manifest in a multitude of ways, such as self-governance, pure and simple exercise of power, or the privilege of power. Thus, there is a reversal of assumption from having greater political autonomy to protect citizens to making a claim of autonomy over society.

This is done regardless of the very citizens that were supposed to be safeguarded, if not in opposition to them. In particular, it seems that our culture shows a lack of systematic reflection on the role and identity of the judge and the professional dimension of judging. Two simple questions always arise in the ethics of judging: "who is a good judge?", "is judging a profession?", questions that could help us to assess to what extent the current judicial set-up may not receive an effective critical stimulus from the emergence of digital justice itself, avoiding most of these declining mechanisms.

The growth of social expectations in the protection of fundamental rights, the rapid technological changes, the slowness and inefficiency of legislative systems, the trans-nationalisation of legal flows, the overbearingness of organised crime, the increase in wealth with the growth of speculative mechanisms and the tendency to corruption, and the intrusiveness of the market, have placed a burden and responsibility on the judiciary that is unprecedented in history.

The increase in the power to intervene in social spheres imposed from outside has been matched, to a greater or lesser extent in the various countries, by a centralisation of power within and a progressive isolation whereby the exercise of justice now appears to be the prerogative of a *small and highly specialised intelligentsia*[6].

If we are to set aside the ideal of the good judge, in order to rely on the mystique of the contest and the technical skills of a bureaucrat, there is less and less reason to reject the mathematical rigour of an algorithm. The impetus provided by the digital alternative could lead to an overall rethinking of the situation before us, imposing a radical reflection on how far the ideal of an exercise of justice guaranteed by human wisdom is increasingly out of touch with reality.

The algorithms of digital justice record and do not "listen"; they are adept at syntactic reconciliations, but indifferent to semantic subtleties; they are unable to empathise with the human condition; they are affected *by* the biases of unknown programmers; they are not transparent, because the technology at our disposal often does not allow

5. Lanza 2011, p. 367. De Tocqueville already posed the problem: "Should the jury, which represents society, have more power than the very society whose laws it enforces?" (de Tocqueville 1840/1968, p. 297).

6. Van Caenegem 1991, p. 137.

us to understand how certain effects are produced (*black box effects*). As Luhmann teaches, social systems also produce *black box effects*: "they develop forms of access to complexity that are not accessible to the analysis of scientific simulations"[7].

We should, first of all, put aside the man/machine dualism to make a comparison between the shortcomings of a corporation, because the difficulty in stemming the growth of corporate tendencies in the judiciary is undeniable, and the limits of a digital system. If that of the judges were increasingly "their" justice, it might be useful to ask ourselves to what extent it would be possible to correct this distortion by starting to rely on an alternative system in the hypothesis that it would be able to recover the essential function of settling disputes in a swift and certain manner, without fuelling the privileges, ambitions and arrogance of power that are characteristic of human organisations.

Faced with the obvious limitations of computerised automatisms, we run the risk of ignoring the equally obvious limitations of our institutions, constructing an abstract image of human capabilities. All the most pressing expectations and the most intense aspirations placed in the anxiety for justice have poured into the figure of the judge, rejecting the idea that he is a bureaucrat among others. These are unintended consequences resulting from the fallibility of human nature: the politicisation of the judiciary, an excessively limited approach towards performing one's obligations, the sluggish pace of trials, aberrant use of procedural tools (such as pre-trial detention and telephone and environmental interceptions), the desire for visibility (ranging from a wish for self-promotion to the continued infringement of investigation confidentiality), and the excessive power of the public prosecutor's office.

The digital judge will always be far from the "good judge", if we idealistically think that the sentence is the nexus "by which the order is welded to life and realised as life". Experience, however, confronts us with a very different reality in which the flaws, rather than the merits, of human actions often emerge. Bureaucratic repetitiveness fosters indifference and irresponsibility fuels self-reference. Moreover, the current set-up of our judiciary does not seem to seek virtue or even presuppose it. This is why we must not reject the hypothesis of a justice entrusted, at least in part, to algorithms.

We must free ourselves from the "anthropocentric" prejudice whereby we imagine a world of machines that act and think like us. These are artificial entities absolutely different from our nervous system and yet preordained to participate in "affective" dynamics with human beings on the basis of extremely complex data reconnection models to which ethical codes will have to be incorporated and refined over time.

The co-evolution of humans and actual social robots will necessarily include a dimension of ethical invention, innovation and "discovery": since law is not "olympic philology", we can expect from a computer an extraordinary capacity for data reconnection, but it is difficult to assume that it would know how to go beyond this technical accuracy. We would have "a deciding without judging", an *agere sine intelligere*. Is this a risk or an opportunity? We can approach this problem from two perspectives, either by claiming the specificity of human sensitivity and creativity as opposed to the aseptic automatisms of a delegation to machines, or by analysing the way in which, today, the judicial apparatus as a whole responds to the fundamental needs of society and protects fundamental rights.

That is to say, we can make an individual assessment of human capabilities or a "system" assessment, comparing the merits and shortcomings of the activities that we attribute to the entity "judiciary", as a complex and self-referential organism, with the possible positive or negative aspects of a combination of algorithms.

For our purposes, we can define AI as the technology that enables a computer to analyse large amounts of data and, on the basis of the knowledge and experience gained, adopt intelligent behaviour or propose decisions. In other words, it is a technology that enables a machine to perform functions traditionally only recognised as human capability[8].

7. Luhmann 1990, p. 81.

8. Boden 2018, according to whom AI is the technology that seeks to "make computers do the sorts of things that [human] minds can do". Cf. also Goodfellow–Bengio–Courville 2016, p. 9.

Among the many technologies that may fall under this broad definition, those based on self-learning systems or "machine learning" are particularly relevant[9]. Every computer operates on the basis of algorithms, i.e., mathematical instructions (or codes) that are used to solve problems, answer questions or perform certain functions. In contrast to traditional computers, which operate on the basis of algorithms or codes established by the programmer, and which can only be modified by the programmer himself, the new "machine learning" systems continuously and automatically derive algorithms that will then be used in their own operation through statistical analyses of large quantities of data. The main feature of the new AI systems, therefore, is that they operate autonomously. The new "robotic" systems, it has been observed, could help to satisfy that need for "calculability of law", pointed out by Max Weber and taken up by those who consider it indispensable to guarantee the citizen's trust in legal certainty[10].

The replacement of judges by automated predictive justice tools, however, raises numerous questions, on which a wide-ranging debate is open[11]. However, there is a widespread need for tools to make the outcome of legal disputes more predictable. Notwithstanding the widespread awareness of the impossibility of entrusting to a machine evaluations that the law entrusts to the judge's prudent appreciation, there remains a need to provide citizens with greater transparency on the possible duration and probable outcome of certain disputes, also in order to limit unnecessary recourse to justice. The so-called "robot judge", in fact, is not equipped with conscience, i.e., with metaphysical awareness of the before, the after, from existence in life as an epiphenomenon, and without a neurochemical pattern of feelings that are fundamental to "feeling" the human soul and capturing its weaknesses.

Some initiatives have been taken in other Courts of Appeal, on whose website links are posted, usable by all, to thematic pages aimed at providing indications on consolidated case law regarding frequently recurring issues[12]. On a technical level, the idea that AI can help eliminate or diminish errors or prejudices that can influence the outcome of the decision-making process has long been effectively challenged. According to some studies, the errors, and biases inherent in human thinking can be reproduced and even exacerbated by AI techniques, as confirmed by the COMPAS affair. In fact, the proper functioning of the system can be affected by learning problems, i.e., by the so-called training data. If this data has not been collected correctly or contains errors, the reliabili-

9. Shalev-Shwartz–Ben-David 2014, pp. 34-45.

10. Irti 2019, p. 17 ss. On "legal calculability" and the relevance that jurisprudential precedents may hold IA purposes of "legal calculability" see the contributions collected in Carleo 2017 and Carleo 2018.

11. Casonato 2019, p.101 ff., as well as the numerous contributions collected in Gabrielli–Ruffolo 2019, p. 1657 ff.; see also Celotto 2019; Fasan 2019; Quatrocolo 2019; Solum 2019; Simoncini 2019; D'Aloia 2019. On the evolution of AI systems see Kaplan 2018, p. 14 ff.; Bernstein 1990, p. 19 ff.; Fasan 2019, p. 102 ff. On the need for a specific regulation for robotics and artificial intelligence and the establishment of an independent body for robotics (as hypothesised in the Recommendations concerning civil law rules on robotics, adopted by the European Parliament at its sitting of 27 February 2017) see Stradella 2019, p. 73 ff. On this topic, see also Garapon–Lassègue 2018; Nieva-Fenoll 2019 and there in extensive and updated bibliography on the topic. On this topic see also Dalfino 2019.

12. Project "Predictability of decisions", approved by decree of 5 October 2016 of the President of the Third Civil Section of the Court of Appeal of Bari. The decree entrusted the preparation of the case studies and the drafting of the sheets to the section's trainees and postgraduates, under the supervision of the entrusted councillors or another councillor designated by the President of the section; it reserved the assignment of the topics to the trainees and postgraduates to the President of the section; it established that the work "will be coordinated by the President of the section and the sheets will be approved by the section councillors during the meetings pursuant to Art. 47 quater Ord. Giud, in which the following may be invited to participate: magistrates, including honorary ones, from other sections; magistrates, including honorary ones, from other offices and other levels of judgement; experts in particular sectors being dealt with (road accidents, forensic medicine, engineering, agriculture, etc.); representatives of the Bar or University lecturers".

ty of the results subsequently offered by the system is inevitably compromised[13]. A second factor that may affect the reliability of the results offered by the software may be due to "statistical discrimination", i.e., the existence of influences determined by previously performed statistical surveys.

Discrimination based on statistical surveys is commonplace, even in the absence of AI systems. This is often due to decision-makers substituting missing information with other available data in order to reach a conclusion on a particular issue. However, the Council of State[14] has expressed the most significant praise by overturning the trial judge's approach and highlighting the undisputed benefits of efficiency and cost-effectiveness in administrative action resulting from the automation of the administration's decision-making process through algorithms that are computer-enabled to assess and grade numerous questions.

Systems of this nature enable the administration to accomplish its goals while utilizing minimal resources and streamlining and accelerating the procedural process, in accordance with the constitutional principle of efficient administrative action (Article 97 of the Constitution) and the obligation to guarantee conformity with the principles of administrative procedure (such as transparency, publicity, reasonableness, and proportionality).

It is necessary for the administration to undertake ex ante activities of mediation and interest composition for acts requiring administrative discretion. This includes consistent testing, updating, and improving the algorithm, especially in situations involving progressive and deep learning. In this regard, it is crucial to confirm the algorithm's knowability across all aspects, from its authors and elaboration process to the decision mechanism, its priorities during evaluation and decision-making, and the selection of relevant data[15]. A direct corollary concerns the reviewability of the algorithm by the administrative judge, in order to be able to assess the correctness of the computer process and the logicality and reasonableness of the "rule" that governs the algorithm[16].

Once the possibility of assessing the reliability of an AI system has been acknowledged, what legal obstacles could hinder its application in the judicial sector? The "predictive" software has been extensively under scrutiny and advancement, aiming to establish the likelihood of success or failure of a particular case presented to a judge. To eliminate the prospect of solely implementing robotic judges, it has been noted that, currently, it is impractical to link the vast range of legal facts that require consideration by algorithmic computing's abstract schemes.

The judge, in resolving disputes, does not limit himself to a simple syllogism, but is called upon to make a series of evaluations that often require complex choices that cannot be predetermined a priori. Moreover, it does not appear to be possible, with today's algorithms designed on the quantitative analysis of cases on *big data*, to replace with an algorithm the judicial motivation of the decision,

13. On a technical level, the idea that AI can help eliminate or diminish errors or biases that can influence the outcome of the decision-making process has long been effectively challenged. According to some studies, in fact, the errors and prejudices inherent in human thinking can be reproduced and even increased by AI techniques, as was confirmed by the case of the COMPAS system, an AI programme designed by a private company to calculate people's risk of reoffending and social dangerousness.
14. Section VI, Judgment No. 2270 of 8 April 2019. The principle according to which "the use of computerised procedures cannot be a reason for circumventing the principles that shape our legal system and regulate the conduct of administrative activity" was subsequently reiterated by the Council of State in a number of decisions that confirm, also by referring to textual references, what had already been sanctioned in Judgment No. 2270 of 2019 (see Council of State, Section VI, Judgments Nos. 8472, 8473 and 8474 of 13 December 2019).
15. On this subject, see already TAR Lazio, Sec. III-*bis*, judgment 22 March 2017, no. 3769, which recognised the right of access also with reference to the so-called "source code" of the programme used in the administrative procedure. On the decision see Simoncini 2019, p. 77; Otranto 2018.
16. On the procedural problems arising from the adoption of computerised administrative acts, and in particular on the possibility of contesting the software independently or only together with the final act, see for example Orofino 2002, p. 2256 ff.; Saitta 2003. On the problems arising from the fact that the holder of the public function does not coincide with the computer-programmer who materially prepares the software see Viola 2018, p. 10 ff.

which substantiates the heart of the constitutional permits of the trial and the very impartiality of the judging body.

In this perspective, the Constitutional Court has deemed illegitimate, in various circumstances, decision-making automatisms provided for by the legislature. Ultimately, the use of the IA alone instead of the judge would affect the constitutional ensures pertaining to jurisdiction, such as the effectiveness and fullness of the parties right of defence, the quality of the jurisdictional decision, the judge's ability to bring out the irreducible peculiarity of the facts and to calibrate the decision on them, and the obligation to state reasons.

2. The *Noetics* of Judging

Does the shield of impartiality allow the judge to prevent emotions from influencing his decision, as if it were an impenetrable barrier to emotional impulses while wearing his robe? The most accepted answer in legal science is affirmative, as it grounds rationality as the core of judicial decision-making. At least from the point of view of procedural rules, it is assumed that the influence of emotions is rejected, as they can distort the cognitive process. When impressions, intuitions and feelings creep into the decision-making process, jurists believe that this leads to a deficiency in the proper formation of legal argumentation, a kind of pathology to be avoided and counteracted in the pronouncement of judgment.

In a work written by Forza, Menegon and Rumiati, the roots and outcomes of the cultural context described above are placed at the centre of the analysis[17]. Using the advanced tools of neuroscience and psychology, the book sets out to take an important step: to decisively and convincingly overcome the traditional separation between reason and emotion. In this perspective, Homo Cogitans, the human being who prepares to make decisions, is not conceived as confined within an enclosure impermeable to the influences of the emotions, crushed by a massive and inaccessible rationality. On the contrary, the authors lead us towards a more multifaceted view of the human being, who can integrate reason and emotion into a richer and more complex decision-making process. They recognise that emotions are not strangers or adversaries of reason, but rather essential partners. Emotions are traced back to their role as legitimate and meaningful influences in decision-making, capable of interacting fruitfully with rational thought. This dynamic interaction between reason and emotion, according to the authors, is fundamental to improving the quality of cognitive operations and thus of the decisions taken by Homo Cogitans[18].

In addition to examining intuitionism in its purest form, the portrayal of the judge as an "emotional judge" offers a more comprehensive view of what we might call "virtuous emotionality"; these emotional virtues emerge from a harmonious combination of different psychological dimensions. In the context of this vision, the figure emerges of an individual endowed with a remarkable social intuition that enables him to grasp not only the external aspects but also the mental states of others, opening the door to a deeper understanding of the people around him. However, this ability is not the only characteristic that contributes to virtuous emotionality; self-awareness is also a key element in this equation.

The individual with virtuous emotionality is aware of his emotions and understands the physical sensations that accompany them. This personal awareness helps him not only to understand himself better but also to be more sensitive to the emotions of others. In addition, focused attention with a high degree of concentration on a specific goal is a distinctive trait of the virtuous emotionalist. This ability to focus intensely on a specific goal enables the judge to thoroughly examine complex situations and make well-considered decisions.

In summary, virtuous emotionality is based on honed social intuition, self-awareness of personal emotions, and focused attention. These personal characteristics create ideal conditions for judgement functions, contributing to a deeper and more compassionate understanding of others and facilitating informed and wise decisions.

In the context of "deviant emotionality", Forza, Menegon and Rumiati present us with a detailed

17. Forza–Mengon–Rumiati 2017, p. 244.

18. On the topic addressed by Forza, G. Mengon, R. Rumiati, it is possible to elaborate with: Goleman 1995, p. 368; Ledoux 1998, p. 384.

analysis of the mental states that can lead to miscarriages of justice, with particular attention to the most serious of them, termed "tunnel vision". This condition is characterised by the rigidity of the decision maker's attention, oriented solely in a specific direction, preventing him from widening his field of vision to the surrounding circumstances[19]. This restrictive behaviour can be compared to a tunnel, the outlet of which often leads in the wrong direction. An emblematic example of this dynamic has been highlighted in cases of miscarriages of justice such as the Tortora case and the Rignano Flaminio court case, in which five kindergarten teachers were falsely accused of child abuse and subsequently acquitted with a broad formula. In these cases, mental rigidity and narrow focus prevented an accurate assessment of the available evidence, leading to serious miscarriages of justice.

Another aspect of "deviant emotionality" concerns the so-called "emotional short-circuit". In this situation, the decision maker jumps to conclusions without carrying out any proper rational verification. This behaviour leads to the creation of narratives based solely on limited and immediate information, often leading to erroneous judgements[20]. The cost of such hasty conclusions is high in terms of the reliability of judicial decisions. This type of mental approach facilitates the manifestation of stereotypes and prejudices, which in turn negatively influence the conclusions reached.

In summary, "deviant emotions" represent a scenario in which judicial errors can occur due to biased or hasty decision-making processes. These dynamics endanger the accuracy and fairness of the justice process, underlining the importance of addressing these issues to improve the quality of decisions in the justice system.

The legislature is also fully aware of the dangers that can arise when the judge is influenced by distorted or deviant emotions. Therefore, the legal system has provided remedies such as abstention and recusal to address this issue. These remedies were established to prevent judges from finding themselves in situations where their impartiality is compromised.

Lawyers, on the other hand, are particularly attentive to the emotional style of the judge[21]. They know that the effectiveness of their defences in a trial depends largely on their ability to adapt their strategy to the psychological profile of the judge in charge of the charge. The choice of evidence and arguments to present in court, the technique used in questioning witnesses, as well as the tone and style of their final argument, are all influenced by a careful balance between legal reasoning and emotional considerations. Lawyers seek to adopt an approach that takes into account the inclinations and sensitivities of the judge to maximise the likelihood of obtaining a favourable result for their client.

In this context, understanding the judge's emotional style becomes a crucial element for lawyers, as it directly influences the defence strategy and persuasiveness in the judicial process. This underlines how important not only legal judgement is, but also the management of emotional dynamics in the context of justice.

It is not at all uncommon for newspapers and major national television networks to "report" on trial events related to crimes that shock the common sense of readers or viewers. True, journalists specialised in judicial reporting and TV talk show hosts may not have the same competence as professional magistrates to assess trial matters. However, what may come as a surprise is that it is sometimes the magistrates themselves who comment on trial matters after they have concluded with a verdict.

These considerations are not intended to criticise the judgment, since judicial decisions are not subject to public criticism, but rather to emphasise the procedural regularity and rigorous logical process that the magistrate necessarily followed in his complex work[22]. What rarely emerges from these considerations is the hypothesis just mentioned that, beyond the procedural correctness to which the magistrate must adhere, there may be a risk that he or she has committed one of the so-called

19. Gulotta 2011. On the subject see also: Gulotta 2014; Findley–Scott 2006, pp. 1-17.

20. Maslach–Schaufeli–Leiter 2001, pp. 397-422. On the topic see also: Lustig–Karnik–Delucchi–Tennakoon 2007, p. 14.

21. Brady 2013, p. 216.

22. Bin 2013, p. 112.

"devious errors". These errors of judgement have been well known to decision psychologists for over forty years and represent traps that can be scattered at different stages of the proceedings.

These pitfalls can emerge from the moment the suspect is brought in as a suspect and continue during the course of the trial during the acquisition and examination of evidence, the questioning of witnesses, up to the stage of the judicial decision and the drafting of the motivation. These insidious, often systematic errors can influence the judgement of the magistrate in subtle but significant ways, leading to erroneous decisions that do not reflect the reality of the facts. Awareness of these risks and the need to mitigate them are crucial to ensure justice and fairness in the judicial process.

It is extremely rare for a magistrate to admit to being influenced by emotions during the different stages of judicial proceedings. The professional training he has received often leads him to believe that his conduct must be guided exclusively by rationality. For centuries, emotions were considered in opposition to rationality, creating a dichotomy that limited the full expression of emotions and hindered the achievement of intended goals.

However, thanks to evidence from cognitive science and neuroscience, we have begun to understand that emotions are an intrinsic element in decision-making and judgement[23]. This means that emotions can play a significant role in influencing the perceptions and evaluations of subjects or situations that are to be judged. And this applies not only to judges, but also to all individuals involved in decision-making processes.

Emotions can have a positive or negative impact on our ability to objectively assess situations; they can be an important source of intuition and sensitivity, but at the same time they can lead to errors in judgement when they are too strong or not managed appropriately.

Therefore, while it is important that magistrates receive rigorous training on rationality and the law, it is equally essential to recognise that emotions are an integral part of decision-making and that their conscious management can contribute to more balanced and equitable decisions. In other words, emotions should not be ignored or relegated to the background but should be understood and managed in a way that supports fairer and more accurate justice.

It is undeniable that the magistrate, although trained to follow rational conducts, is also susceptible to the influence of emotions. The question becomes crucial when considering cases of extreme brutality and atrocity, where the evidence presents particularly violent aspects, and the testimonies are charged with emotional impact. In these situations, it is legitimate to question whether the magistrate can remain completely immune to the surrounding emotional wave and possible mental traps.

It is not at all uncommon for some judicial decisions, relating to cases that have become classics, to appear to be heavily influenced by the emotions underlying the human case rather than by an exclusively rational assessment based on the objectivity of the evidentiary data. It is precisely the emotional impact that can guide the judge's decision-making process, pushing him towards options that may not be verbally explicit but that reflect the deep-seated impressions of the object of evaluation.

Under these circumstances, the concept of "intuitive judgements" mentioned by the cognitive scientist Daniel Kahneman, Nobel Prize winner for economics in 2002, becomes relevant. These intuitive judgements are not necessarily the result of a rational and objective process, but rather reflect the individual's impressions and affective feelings about the situation[24]. Judges, when called upon to make decisions, may incur "biases" (preconceptions), "thinking heuristics" (simplified mental strategies) and, in general, cognitive traps. These influences may stem from the emotions and affective feelings that arise during the decision-making process. Recognising the importance of these

23. Fiandaca 2013, p. 215.

24. Kahneman 2012. Other relevant works by the author on the subject are: *Prospect Theory: An Analysis of Decision under Risk* (1979) – This is one of Kahneman and Tversky's most famous articles, in which they presented the prospect theory, which revolutionised the understanding of human decision-making under uncertainty; *Judgment under Uncertainty: Heuristics and Biases* (1982) – Another fundamental article written with Amos Tversky, which introduced the concept of heuristics and biases in decision-making.

dynamics is crucial to better understand how to improve decision-making and promote fairer and more balanced justice.

3. *Legal constraints* for a non-human judge

If our constitutional principles preclude, but only at present, entrusting the exercise of the judicial function to a legal machine, it is, on the other hand, possible to hypothesise the use of AI in an instrumental and auxiliary function for the judge or its multiplication. For instance, modern AI systems could certainly facilitate the activity of searching for precedents.

They could, that is, provide new and more powerful search engines that would enable litigants to assess whether or not to initiate a trial, and the judge to more easily find the framework of precedents that can be used for decision-making purposes. Indeed, there is an emerging need to adapt traditional legal categories to a new reality, in which many decisions are taken not by human beings but by algorithms that can make unpredictable choices.

The new "robotic" systems, it has been observed, could help satisfy that need for the "calculability of law", pointed out by Max Weber and taken up by those who consider it indispensable to guarantee the citizen's reliance on legal certainty[25]. For example, it has been proposed in doctrine to provide for a preliminary phase before the commencement of a judgment, based on the use of an AI system, aimed at establishing the probable outcome of the judgment.

The parties would have to decide whether to accept the immediate robotic decision or to proceed before the court with a different time frame. In such a case, the losing party for not having followed the AI system's "suggestion" should, according to the proposal, be ordered to pay damages for reckless litigation under Article 96 of the Code of Civil Procedure.

In addition, the use of the new AI tools could prove valuable in the application of the new "appeal filter" mechanism, which requires the College to declare inadmissible an appeal that does not have a "reasonable likelihood" of being upheld[26], just as it could prove to be a valuable tool, for instance, to quickly make compliant precedents available to the adjudicating body, for the possible referral of the decision to the United Sections – in a faster and more efficient manner – the activity of "perusal" of judgments for the purpose of applying the admissibility filter for appeals to the Court of Cassation or Appeal[27] (in these cases the final decision as to the admissibility of the appeal would still be left to the judge).

AI systems could, moreover, offer an aid in any case in which it is necessary to make technical evaluations aimed at determining monetary amounts in the context of civil judgments also to reconstruct factual data to be used for decision-making purposes, or for the preparation of draft orders or for the handling of simple, serial, repetitive, entirely documentary cases, within the limits allowed by the applicable legislation.

The use of new information technologies could also, "if properly governed and accompanied by professional and training measures, assist policies to improve the efficiency of judicial governance". Finally, AI systems can be used in alternative dispute resolution procedures, including, for instance, those involving so-called *small-claims*, i.e., matters of bagatelle or low economic value that would be unlikely to be enforced before a judge. Part of the doctrine, however, still seems to be highly sceptical about the possibility of allowing judges to use AI tools, especially if they are predictive in nature, to support their decisions.

25. Irti 2019, p. 17; see also the contributions collected in Carleo 2017 and Carleo 2018.

26. Article 348-*bis* of the Code of Civil Procedure (c.p.c.), introduced by Law Decree No. 83 of 2012 converted into Law No. 143 of 2012. Art. 384-*bis* c.p.c. would legitimise predictive justice algorithms as a consequence of law, because it sanctions with inadmissibility the appeal that does not have a reasonable probability of being upheld, thus sanctioning the use of probabilistic automated decision-making processes for the purposes of the judge's decision; but this is denounced by Art. 22 of GDPR 679/2016 which states: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar way". Higher-ranking European norm derogates from the lower one given by Art. 384-*bis* c.p.c.

27. De Renzis 2019, p. 150.

The problem, it has been observed, relates to the "overwhelming practical force of the algorithm", which would end up inducing the judge to follow the choice suggested by the computer, thus ending up conditioning its motivation.

The risk posed by the adoption of AI in the decision-making process is that the data offered by the "intelligent" instrumentation would no longer have an indicative or persuasive value, but an almost prescriptive one, causing the operator to apply the solution offered by the machine without examining it in the light of the particularities of the concrete case.

In other words, if the judge, in deciding, were to end up uncritically resting on the algorithm's proposals, the mechanical reproduction of decisions would risk leading to a dangerous crystallisation of jurisprudence to the detriment of its evolution. Such risks must be decisively avoided.

The autonomous assessment of the judge, who is exclusively responsible for the interpretation of the applicable law and the assessment of the peculiarities of the case at hand, is, above all, to be regarded as an inalienable social value. Once an automatic decision-making system has been introduced into a human decision-making process, it has been observed, "the automatic system tends, over time, to capture the decision itself", also in view of the "practical" force of any evaluative automatism that, on the one hand, relieves the decision-maker of the burden of motivation, the burden of examination and motivation; on the other, allows him to "qualify" his decision with the chrism of "scientificity" or "neutrality" that today surrounds algorithmic evaluation and confers on it a peculiar – how unfounded – authority[28].

The mere *tout court* substitution of the judge (but not his cloning) with AI systems cannot, however, currently be admitted in the Italian legal system, because it is contrary to constitutional principles, this, above all, because the Constitution was constructed not as a balance between values, with the consequence of favouring subjectivity over objectivity and, therefore, the human being over "other".

Article 102 of the Constitution, which entrusts the exercise of the judicial function to magistrates established and regulated by the rules on the judicial system, and Article 111 (due process), second paragraph, of the Constitution, which requires every trial to be held before a third and impartial judge, postulate a human judge. Article 101, paragraph 1 of the Constitution, in providing that judges are subject only to the law, excludes that the judge can be bound by the outcome of algorithmic procedures that place the legal practitioner in front of dangerous application automatisms.

Article 25 of the Constitution itself, in guaranteeing the right to a "natural judge pre-established by law", evidently refers to a judge-person. Article 51 of the Code of Criminal Procedure (abstention of the judge) postulates, unequivocally and perhaps more than others, the human nature of the judge; in this article, observing the trial as a whole, one can infer a principle of symmetry between judge and parties, in the sense that they must have the same human nature, differing only in role and/or power. These provisions clearly exclude the possibility of an artificial intelligence system replacing the judge.

The replacement of the judge by automated dispute resolution mechanisms would, moreover, compress the parties' right of defence. A robot judge, of deontic implementation, always needs a robust logical-legal theory to demonstrate its ability to issue "just" judgments by virtue of automated algorithms with a broad consensus, which would seem to undermine the recognition of a particular status – such as that of a legal subject – to a robot judge.

The EU Parliament resolution of 16 February 2017 recognising the importance of the world of robotics and artificial intelligence in need of regulation is concerned about this. The guarantee of every citizen's right to an independent and impartial judge is moreover also reaffirmed by the ECHR (Art. 6(1)) and the Charter of Fundamental Rights of the European Union. In this perspective, the *Committee of Experts on Internet Intermediaries* of the Council of Europe published the study *Algorithms and Human Rights* in March 2018.

In view of the "growing importance of AI in modern society" and the "expected benefits once

28. Simoncini 2019, p. 81. See also Barbaro 2018, p. 194, according to which the use of predictive tools could have repercussions on the impartiality of the magistrate, given the likely reluctance of judges to shoulder the burden of deciding against the prediction of an algorithm.

its potential is also used to serve the efficiency and quality of justice", a few months later the European Commission for the Efficiency of Justice (CEPEJ), established by the Committee of Ministers of the Council of Europe, adopted the *European Ethics Charter for the Use of AI in Justice Systems*[29].

The Ethics Charter sets out some basic guidelines for "public and private actors responsible for the design and use of AI tools and services". The basic idea that emerges from the Ethics Charter is that AI, if used as a tool not to replace, but to assist the judge, can, in certain circumstances, promote predictability in the application of the law and uniformity of jurisprudential orientations.

This is the first instrument in Europe that identifies the fundamental principles to which the use of AI in judicial systems should adhere: respect for fundamental rights, non-discrimination, quality and security of the system, transparency, and user control. Compliance with these principles should be ensured right from the design and learning phase of the system, according to an "ethical-by-design" or "human-rights-by-design" approach. Compliance with these principles should be ensured by an independent authority with certification and monitoring tasks.

The Charter contains, in an appendix, a study on some AI applications being tested in some European states, a recommendation on the use of such applications, a glossary and a self-assessment checklist, aimed at enabling a check on the level of adherence to the principles set out in the ethical charter. Although the Ethics Charter is non-binding in nature, it is called upon to play a guiding and guiding role in ensuring that AI systems, from the design phase to practical application, guarantee respect for fundamental rights and data protection regulations.

Finally, in this context, it is worth mentioning the Artificial Intelligence Regulation (AI Act), which is a binding legal instrument that expands and concretizes many of the principles already enunciated by the Charter of Ethics. The AI Act aims to create a regulatory framework that regulates the use of AI in a manner proportionate to the risk that such technologies may pose to fundamental rights, security, and democratic values.

This regulation aims to strike a balance between technological innovation and the need to protect fundamental rights, security, and democratic values. In a context where AI plays an increasingly pervasive role in society, the AI Act aims to prevent the risks associated with these technologies by ensuring that they are used responsibly and transparently[30].

A central aspect of the AI Act is its risk-based approach, which classifies AI systems into four main categories, depending on their impact on fundamental rights and safety. This classification allows rules and obligations to be calibrated in a manner proportionate to the level of risk, thus ensuring a balance between technological innovation and the protection of fundamental rights.

The AI Act, therefore, not only seeks to reduce the risks related to AI but aims to bring about innovation. By establishing clear and consistent rules at European level, the regulation aims to create an environment of trust that incentivizes the development of safe, ethical, and human rights-respecting AI solutions.

4. Communication meta-referents for *robotic judgement*

The legal system is not reducible to a pure biological system, i.e., of mere living forms and devoid of questions about the meaning of before and after and the metaphysical why of life. The genealogy of law represents law as bound to the relationship of unconditional and universal recognition between men, which overcomes that of exclusion, based on pure factuality, and a legal relationship allows for the reciprocity of the encounter, recognising and preserving the originality and uniqueness with which each individual is branded from his or her origins.

When then, the rational human process acts in a theoretical sense as a source of obligation and moral authority, it becomes a norm for every human being. The legislation of reason is finally exhausted in a single rule operating with the formal

29. A few months later, the European Commission for the Efficiency of Justice (CEPEJ), established by the Committee of Ministers of the Council of Europe, adopted the *European Ethics Charter for the Use of AI in Justice Systems*.

30. Iaselli 2024, p. 436.

and selective criterion of universal law. Coercive actions become legitimate only when they are necessary to the logical consequences of actions that, through an invoked legal principle, are recognised as necessary and, therefore, assigned as a legal duty.

The fulfilment of legal law thus legitimises itself as the primordial condition of categorical imperative, specialising in the conformation of duties that can be demanded by force. While in its moral form, it demands that we act according to sayings and adages that can likewise be expressed through their validity as ethical laws, in its legal form it is represented as the principle of what is logically just. Law thus becomes an indispensable tool for organising correct social relations, preventing the onset of social conflict that could arise from the concentration of at least two different appetites on the same "good-life", or, should the conflict arise in any case, restoring, through the application of the legal rule, that social order disturbed by the head-on clash of the two competing and opposing appetites, which confirm the inseparability of law with the anthropic society that generated it.

If law is always constituted of utterances and propositions that, in terms of communicative intentionality, assume functions relative to the purposes that the speaker proposes to achieve, the task of legal logic is the study of *lógos*, of legal thought and language, as a search for rationality and logic in utterances with normative value. While logic claims to formalise its research products in a logical language with Boolean functions, law does not operate on a purely syntactic level, i.e., by means of series of symbols or rules of logical elimination formation, but accuses its own semantic domain[31], in order to explicate certain legal entities with rationality and to account for the behaviour as a logical sub-species of these entities in the legal universe[32]. Indeed, in logic, conditional modular structures are used with mixed modes: alethic; deontic; epistemic; these modes always present the character of "provisionality, vagueness, paraconsistency, non-monotonicity, polyvalence"[33].

Kelsen argued in this regard that "there is no need for special logics to account for judicial decisions"[34], which contrasts with the position of those who hold, on the other hand, that classical logic is not sufficient to account for the rationale of legal reasoning[35] at least in the motivation part of the judgment. At present, it is clear that artificial intelligence lacks the ability to exercise discretion and make judgments. To evaluate the compatibility of AI with the deontic logic of decisional legal reasoning in the context of digital expression, it is important to note that the question remains purely theoretical, and that there is still much to learn about cognitive sciences. It is necessary to observe, however, that the use of a typified logic of the information process could be a potential area for AI application[36].

A robot judge, of deontic implementation, requires, as anticipated, a robust logical-legal theory that demonstrates its ability to make "just" judgments by virtue of automatic algorithms with a

31. An idea that is provocatively supported, also in relation to manipulation by computers, by: Alchourrón–Martino 1990, p. 25.

32. The language of law has a structure open to hetero integrations since it expresses statements that, in principle, can be integrated. There can only be integration if the utterances are capable of revision and if its truth values are rooted. Law is always constituted of utterances and propositions that, in terms of communicative intentionality, assume functions relative to the purposes that the speaker sets out to achieve. The task of legal logic is the study of lógos, of legal thought and language as a search for ratio in statements with normative value. While logic claims to formalise its search products in a logical language with Boolean functions, law does not operate on a purely syntactic level, i.e., through series of symbols or rules of logical elimination formation, but accuses its own semantic domain, in order to explicate certain legal entities with rationality and to account for the behaviour as a logical sub-species of these entities in the legal universe.

33. Hughes–Cresswell 1996.

34. Mazzarese 1996; Alchourrón–Martino 1990, pp. 46 67.

35. Kelsen argued in this regard that "there is no need for 'special logics' to account for judicial decisions", which contrasts with the position of those who hold, on the other hand, that classical logic is not sufficient "to account for the rationale of legal reasoning" at least in the motivation part of the judgment.

36. On this subject, Sartor 2003.

broad consensus, which would seem to prejudice the recognition of a particular status – such as that of a legal subject – proper to a robot judge. In the words of Giovanni Sartor, "man is naturally inclined to apply to artificial entities, and especially to A.I.'s, those interpretative models that normally apply between human beings, particularly by explaining the behaviour of given entities by attributing to them mental states proper to human mental mechanisms, precisely"[37]. Such a reference to humanising mental states would entail a behaviourist application to be adopted specifically for artificial entities[38].

The path of further study, which is being taken by frontier legal informatics, concerns the interpretation of neutral and flexible mental concepts, applicable to special categories of artificial entities, allowing the preservation of the unity of law for an automated information process[39]. Without addressing the potential psychic and cognitive mental states, the issues regarding granting legal subjectivity to AI can be resolved using two theories, namely Savigny's theory of fiction. The concept utilises a legal fiction to confer subjectivity upon non-human social entities, particularly beneficial in the case of automata which cannot be classified as humans or personal property.

Gierke's theory of legal reality assigns subjectivity to social entities that demonstrate traits similar to humans, indicative of a sociological identity and consciousness. This second theory upholds the legal status of automata, recognizing their similarity to human beings to a greater extent than social bodies. Both theories were eventually superseded by the dualistic case theory, thus opening up new avenues for the recognition of legal subjectivity by the legislature but also limiting itself to the recognition of an instance manifested in time[40].

If logic[41] claims to formalise its own research products in a logical language[42] with Boolean functions[43], law does not operate at a purely syntactic level, i.e., through series of symbols or rules of logical elimination formation, but accuses its own semantic domain[44], in order to explicate certain legal entities with rationality and to account for the behaviour as a logical sub-species of such entities in the legal universe[45].

In the search for the connection of the logic of language to the analysis of the mind, Russell[46] introduces the concept of "propositional attitudes", i.e., the attitude of a subject towards the proposition, as a representation of the meaning to be shared between different utterances, as the connection of a particular written or uttered utterance with the state of mind that induced that particular utterance itself, as Searle put it[47].

Quine posits that the indeterminacy resulting from our capacity to translate disparate linguistic expressions into a singular concept exemplifies the fallacy of positing the existence of mental states that manifest intentionality as a tangible phenomenon. Consequently, the behaviourist analysis of human behaviour can be reduced to a simple holistic interpretation. Quine argues that the indeterminacy resulting from our ability to translate diverse linguistic expressions into the same concept demonstrates the fallacy of believing in the existence of mental states that are indicative of intentionality as a tangible phenomenon. Consequently, the behaviourist interpretation of humans can be

37. Sartor 2005.
38. *Ivi*, p. 4.
39. *Ibidem*.
40. In this regard, the EU Parliament resolution of 16 February 2017 recognising the importance of the world of robotics and artificial intelligence in need of regulation.
41. Strawson 1961.
42. Agazzi 1980.
43. Mangione–Bozzi 1993.
44. An idea that is provocatively supported, also in relation to manipulation by computers, by Alchourrón–Martino 1990.
45. Wittgenstein 1967.
46. Russell 1914.
47. Searle 1984.

seen to amount to a straightforward holistic explanation, as put forth by Davidson[48] and Putnam[49].

Finally, Ryle[50] distinguishes between the physiological processes that occur in the individual for which physiological vocabularies are used and the mental vocabulary that is adopted to communicate behaviour, so much so that Wittgenstein[51] remarked on the possible emergence of linguistic confusion. Mental terms, such as justice, punishment, reward, are for Ryle and Wittgenstein objects of learning in a public context. However, it is difficult to identify the precise point at which intentionality emerges as a precursor to behaviour in everyday life, as mental terms do not necessarily cause behaviour. Furthermore, mental states are also intertwined with behavioural states, making it challenging to distinguish between them. This difficulty is reflected in the legal world, particularly in the penal system, which employs the τετρακτύς ideation-preparation-execution-consummation model for crime[52].

The fundamental rule used by the human race to illustrate the individual behavioural perimeter stretching towards the area of collective coexistence is the linguistic act *tout court*. Many linguistic acts do not merely reflect the state of the world but rather aim to transform it in accordance with the contents of the linguistic act. When a judge orders witness testimony or hires a professional to provide expert opinions, or when a prosecutor assures the victim of a wrongdoing of their intervention to prolong the investigation to find the perpetrator, the aim is not to state the objective truth of the world but rather to change it through a linguistic act intended to effect change.

When the purpose of the order is to produce obedience, the promise, on the other hand, drives one to cause its fulfilment. In these cases, the purpose formed by the linguistic act is not already an agreement with a reality existing independently of it, rather, it aims to change reality so as to adapt it to the content of the linguistic act. If one promises to contract marriage, the aim of this utterance will be to produce a change in the reality of the conjugands, creating a reason for the utterer to contract marriage, which induces the promisor to keep his promise.

If one orders anyone to present themselves in court, the aim is to induce them to present themselves by virtue of obedience to the precise order, to allow their behaviour to harmonise with the content of the linguistic act: the world must change to correspond to how it is described in legal language by an order, and orders are not true or false, but obeyed or disobeyed.

In this sense, the language of law, which translates categorical imperatives into linguistically competent forms of principles of justice, represents the communicative expression of precise needs of society, formalised in the verbalisation of collective wills that is expressed in the brocardo *ubi societas ibi ius*[53]. The juridical language thus appears to be one of the languages with the most tradition and tetragonous to modernisation, inasmuch as "with respect to the changing influences and linguistic fashions found in technical-scientific languages, the juridical lexicon […] has remained fairly stable over time. […] The social prestige of the language of law is ancient; it is an expression of power and institutions and is part of the connective tissue between law and behaviour, thus, between the abstract norm and the citizen"[54].

The language of law, however, is also the same natural language that is uttered by people, so it is a conventional language rather than a formal language, that is, it is entirely natural and as such it is affected by common linguistic polysemies and the different functions they perform. The language of

48. Davidson 1980, pp. 207-224.

49. Putnam 1987.

50. Ryle 2009.

51. Hadot 2007.

52. Mittermaier 1846, p. 265.

53. In Aa.Vv. 1986, p. 7. *Ubi societas ibi ius* is a Latin locution meaning "where there is a civil society, there is law". Every society can only be rooted in law and no civil society exists without self-regulation. The locution is derived from the full sentence: *Ubi homo, ibi societas. Ubi societas, ibi ius. Ergo ubi homo, ibi ius*, a principle of Romanesque origin indicating that man needs legal rules to be able to live.

54. Trifone 2009, p. 265.

law and its transformation into law, touches almost every aspect of the citizen's life through laws and acts of legal relevance, according to the principle that *ignorantia legis non excusat*: the language of law, that is, becomes the language of all, without distinction, and the social actor constantly performs legal activities, such as buying property or renting a house, and in performing these actions uses the language of law. By extension, the language used by the judge can be seen as a means of pacification and conciliation to put an end to disputes between cives, *so it must be* made comprehensible.

Legal language therefore has a fundamental function for mankind precisely because it is directed to all members of the community to regulate acts, facts, and events. The language of law has a structure that is open to hetero integrations because it expresses statements that, in principle, can be integrated. There can only be integration if the utterances are capable of revision and if its truth values are entrenched. At this stage, the statements of law are ratified as standards, which means they create a specific connection between human conduct identified based on a fact and society's response in the form of a positive or negative sanction. In certain cases, new social practices are created, resulting in the formation of social facts. The rules of physics, referred to as norms, also play a significant role in producing social reality by identifying facts which then lead to a precise set of consequences. In certain cases, new social facts are created, i.e., "practices" are produced[55] and the norms, like the rules[56] of physics[57], produce a "social reality", i.e., they identify "facts"[58] i.e., they identify facts from which a precise set of consequences follows[59].

5. Algorithms for *Robotic Justice*

Words, therefore, guide actions, directing behaviour and, thanks to effects known as *priming* and *nudging*, partisan legal acts can guide judgmental action, and judgmental action is described in the legal act par excellence that is the judgment. The *priming* effect[60] is the phenomenon whereby exposure to certain stimuli guides humans into subsequent behavioural types referable to the same domain as those stimuli.

The *nudge* effect[61] alters people's behaviour in a predictable way, although apparently without

55. Viola–Zaccaria 2003.

56. Schauer 2000.

57. von Wright 1989.

58. Searle 1995.

59. Hart 1961; Ross 1965.

60. *Priming* is an unconscious mnemonic recognition by primitive exposure, which allows a stimulus, even a primitive one, to be identified during subsequent evocative exposures without having any awareness of it, posing severe problems on the interpretation and evaluation of the information received. In English, to prime means to trigger that is, to activate a series of information mechanisms present in memory, predisposing and facilitating the subject in the cognitive processing of the next stimulus. Priming makes use of the heuristics of recognition, whereby each piece of information is stored in a mental schema formed temporally on successions and linked to information flows received with respect to the first piece of information acquired. During the priming effect, each subsequent stimulus increases the accessibility of information in memory. According to neuropsychology, priming consists of the activation of groups of neurons surrounded by weak connections between them, so that when these neurons are activated by the perception of an object already seen, the signal immediately spreads and becomes prioritised over the others coming in. This activates a memory in the implicit memory that influences the response, and which represents the incoming information; thus, a series of images related to the object in question is activated in our minds. By repeatedly exposing people unconsciously to a stimulus, i.e., by means of "subliminal perception" a greater positive attitude towards the stimulus to which they are exposed is obtained and the greater their new exposure to the stimulus will be, like a kind of "stimulus hunger". Finally, in order to increase accessibility to information through priming, the purpose must manifest itself as immediately available, otherwise priming alone fails to dictate that people do things they do not want to do. It is amply demonstrated by neuropsychological studies that one cannot induce aims and goals in subjects if these are not already present in their imagination.

61. The theory of nudges people towards behaviour that is positive for their well-being, without using coercive methods but leaving them free to choose: the decision-making processes and behaviour of groups and individu-

prohibiting the choice of other options and, in any case, without significantly changing their value and economic incentives within the scope of individual choices. Judicial *opting out* entails the acceptance of consolidated and tested mental schemes formed by the processes of *priming* and *nudging*: such tools find a secular collocation in "collections", "compendia", "maxims", "pandettes", "codes", but, above all, these are formed as legal documents, understood as private extra-procedural writings certain in terms of paternity and provenance or acts of various kinds at the disposal of the judge that form his opinion and mature his decision.

This Skinnerian stimulus-response-reinforcement cycle[62], rather than the habit loop (signal-routine-gratification)[63] responds better to the formulation and realisation of a protocol of algorithms to produce clones of the monocratic judge.

This protocol is formulated from the theories of language and communication unanimously recognised by the Italian and international scientific community[64]. What is represented is not the replacement machine of the judgement-maker, but rather its clone, that is, the exact judgement-maker multiplied. The robotic machine would not be just any judge, but that very same judge to whom the case would be assigned and who would therefore assume its legal mentality, preparation and human, eventual and always undesirable ideological entrainment.

The first problem to be addressed in preparing a protocol is given by the analysis of anthropic communication in a theoretical sense, the study of its entropic evolution, even to the realisation of an error-free syntropic judgement model. Finally, starting from the judgements of the judge by means of a reduced statistical model, broken down by the legal institutions dealt with by the judge, design the customised judgement-type.

Upon entering into the entropic calculation of the sentence text, it becomes evident that the calculation of the entropy of a linguistic text, whether

als can be influenced through "indirect" suggestions and reinforcements with an effectiveness equal to or greater than that which can be obtained through the imposition of rules, laws or direct instructions: the desire to feel accepted, to be part of a homogeneous group that shares ways of thinking, values and behaviour is a natural need for human beings. Social pressure is, therefore, a very effective weapon that can drive people to conformism, discrimination and the adoption of bad habits, but also to virtuous behaviour, cooperation and activism. Communicating or, even better, showing how many people have made the same choice or implemented the same behaviour increases the likelihood that others will "follow suit". human beings naturally manifest an aversion to change and a tendency to inertia. For this reason, the use of "default options", i.e., default settings, is very effective in guiding an individual's choices. Offering the individual a recommended or directly pre-set option is tantamount to lowering the cognitive load required to make the decision; consequently, in the absence of a strong personal motivation, most people will tend to accept it passively.

62. Learning in a three-term contingency (discriminating stimulus, behavioural response and reinforcing stimulus) occurs following the issuance of a single response, in a manner that can be described as discrete or all or nothing. Teaching technologies, from a perspective consistent with B. F. Skinner and Murray Sidman, therefore, do not require the person to go through an error phase in order to learn something. Errors can be avoided, and with them a number of side effects of punishment, if the teaching technology is designed on the basis of shaping both behavioural responses and discriminating stimuli (response shaping and stimulus shaping) according to the paradigm known as errorless learning).

63. The habit loop has always been used in behavioural psychology in operant conditioning, where a learned behaviour is maintained by the responses it receives. The habit loop consists of three phases: the signal: the consequence of a particular condition (environmental, emotional, …) that requires a gratification, and prompts the brain to perform the routine to obtain it; the routine: the action that occurs following the occurrence of the signal. A routine can be physical (action performed), mental (thought) or emotional (change in mood); the gratification: the reward obtained from the performance of the routine. It is the element that reinforces the unfolding of the ritual of habit.

64. Cf. writings by: Gopen-Smout, De Mauro, Cortellazzo-Viale, Sabatini, Mortara-Garavelli, Rovere, Ondelli-Romanini, Pellegrino, Zaccaria, Timpanaro, Guastini, Belvedere, Dell'Anna, Viezzi, Ainis, Romano, Reinach, Austin, Cohen-Perrault, Habermas-Honnet-Joas, De Fazio, Masini, Simone, Voghera, Abutalebi-Green, Shannon, Manfrino, Minnaja-Paccagnella and many others.

it be a newspaper article, a novel, a poem, or an article of law, is at least a quarter of a century old[65]. An entropic calculation was made at the end of the 1990s based on grapheme frequency tables drawn up for some European languages[66]. This led to the development of an entropic theory of communications, which employs mathematical-statistical source models endowed with the Markovian[67] property to test the intelligibility of a message. These models can be simulated by means of a computer[68].

The limitation of this approach appears to be associated with the evolution of language over time[69], which could potentially result in a reduction in entropy. It is evident that, as was the case previously, the entropy calculated at the grapheme level varies in accordance with the lexical components of the text under consideration. However, this variation, which is relatively limited, tends to diminish with an increase in the length of the selected text. Conversely, if entropy is calculated at the level of phonemes, it varies considerably according to the chosen phoneme transcription.

Additionally, entropy is a quantitative measure of the degree of disorder within a system. It can be conceptualised as a metric that represents the proximity of a system to a state of equilibrium: "This is evidenced by the observation that all entropic phenomena, whether physical or linguistic, tend to evolve towards a state of uniformity. In other words, they proceed from a differentiated state towards a more homogeneous and simple state. As time passes, the system becomes increasingly homogeneous and uniform, which is to say that the entropy of the system itself increases"[70].

The entropic communicative world is inherently a representation of assertions based on incomplete information. It is the result of the "…interaction of individuals, and as such, it is inherently unpredictable. This unpredictability results in a high entropy, which can be defined as one of the possible states of "consistent"[71]. The *de facto* unpredictability of individual human behaviour, as a result of the self-referentiality of homo socialis[72] and the variants of the logic underlying our free will, gives rise to unpredictability in legal computation. This can be attributed to the chaotic nature of information in law, which can be defined as the entropy of legal information"[73].

If a legal practitioner offers only one answer to each procedural legal question, and therefore only one measurement, to complementary questions that exclude each other, answers and measurements are offered that elide each other. This results in entropic causality in law being nothing but the result of the limitedness of the information received and produced. Evolution occurs through the "when" and "where" the legal information contained in the norms is activated, as their sufficient condition, and the *Quis, Quid, Ubi, Quibus auxiliis, Cur, Quomodo, Quando* as their necessary and sufficient condition.

A legal programme of "quality" must be "symmetrical", i.e., ordered at its origin. Over time, that which is homogeneous will become chaotic, with a decay that can be slowed down, counteracted, but never eliminated. The need for recodification intervenes for this purpose as decisional reprogramming. As stated by Prigogine and Stengers, "The speed of entropisation can be slowed down but never stopped, and high entropy states are much more numerous and therefore more possible than low entropy states: this is true for any type of organisation of information"[74].

The implementation of potential slowdown systems necessitates the continuous input of both

65. Shannon 1951, pp. 50-64; Barnard 1955, p. 49.
66. Manfrino 1960, pp. 4-29.
67. Battaglia 2007, pp. 51-69.
68. Debiasi–Valli 1968, pp. 293-314; Minnaja–Paccagnella 1977.
69. Afendras–Tzannes–Trépanier 1973.
70. Gintis–Helbing 2013.
71. Lloyd 2006.
72. Gintis–Helbing 2013.
73. Sabetta 2008.
74. *Ibidem.*

human and computer resources, resulting in an entropic reduction. This is achieved by enhancing the information calculation capacity in accordance with Moore's law, while maintaining a constant valuation of available resources. This can be described as the "transfer of entropy from one system to another" or, alternatively, a reduction in the chaoticity of the system on which the legal programme is to operate. The exchange between rules (the legal programme) and energy (the judicial resources) results in information becoming entropy, which is invisible and therefore unusable.

It can be argued that legal information is an inherent and defining aspect of reality, preceding the actuality of the situation. However, the legal information element, or "bit", is defined as a binary alternative between two extremes. This presents a complexity that is only later evaluated as an evolution of information, or its temporally successive elaboration.

One cannot perceive a legal event or any event in and of itself; rather, one apprehends it through consciousness, becoming part of it, attracted by it, and processing it. In other words, one is indistinguishable from the legal event by becoming a normative source in and of itself. Consequently, the entropy of the information content of the individual norm becomes irreversible once its meaning has been altered, as the measurement of information alters the information in contact with the system itself. At this juncture, it is imperative to conceptualise the legal structure as a causal structure, wherein the interpretation of the norm gives rise to the structure of the legal organisation. However, this, in turn, influences the interpretation and the legal reality in a manner analogous to any reality in terms of information processing.

It follows that in order to achieve the desired organisational result, such as a "just" sentence, there are various paths, i.e., various possible recombinations of norms. This is due to the fact that the "… length of information increases the probability of its decoherence…"[75]. Therefore, the shortest reasoning resorted to is that which is probabilistically more exact and given by the *novacula occami*, i.e., the "principle of economy" or "…The principle of parsimony, which indicates that "…among several hypotheses for the resolution of a problem, the simplest one should be chosen with equal results, is a methodological principle"[76]. It is also reflected in the Latin brocardo: "Frustra fit per plura quod potest fieri per pauciora", which translates to "Entia non sunt multiplicanda praeter necessitatem". Finally, the Latin phrase "Pluralitas non est ponenda sine necessitate" demonstrates regularity, structure and order. As a result, the human function is increasingly limited to the mere formulation of material facts, rather than legal facts. This is particularly evident in the decision-making process regarding the interpretation and processing of large amounts of information, in accordance with the aforementioned Moore's law. Consequently, the scope for decisive action is reduced to the simplified codification of events and sentences, in line with Occam's razor.

At the end, the use of mathematical-statistical model-sources with the Markovian property, which can be simulated through a computer, to gauge the comprehensibility of an oriented communicative message in legal communication has limitations. The evolution of language over time may result in a reduction of entropy usually found in court documents representing legal facts. If entropy is calculated at the level of phonemes, it varies considerably depending on the phoneme transcription chosen. Thus, if one wishes to frame it in a study for a simulator, a verbal source synthesising the human voice can be considered a Markovian analogue process of the written verbal source alone[77].

The entropy[78] of an information source provides insight into the minimum number of "av-

75. Carroll 2006.

76. *Ibidem*.

77. Various Authors 1975, p. 296; Various Authors 1974.

78. From the definition of thermodynamic entropy, it can be deduced that there is a relationship between information and thermodynamic entropy. In-depth studies in the field of information theory were initiated in 1948 by Claude Shannon, who enunciated the "uniqueness theorem of entropy" in information theory as follows: A set of alphanumeric characters, A, is defined as {A(1), A(2), A(3), … A(n)}. The probability of observing the symbol A(i) is defined as p(i). The entropy, H, is then defined as H(p(o), p(1), …, p(n)). As can be observed, the entro-

erage" bits required to store a message from the source and the predictability of messages emitted by the source[79]. It has been demonstrated that a sequence of messages emitted by a source can be compressed, without information loss, down to a minimum number of bits per message equal to the entropy of the source. The sequential arrangement of alphabetical letters, such as aaaaaaaaa, exhibits a lower level of entropy than a word like "sentence," which in turn displays a lower level of entropy than a completely random string, such as frhsnr04ns-29450gmd. In general, entropy can be defined as the randomness inherent in a given string of characters. It is closely related to the minimum number of bits required to represent that string without error.

Thus, in information theory, Shannon's formula[80] for calculating information entropy is described by the equation[81]:

$$H(X) = -\sum p(x)\log_2 p(x) \qquad [1]$$

x ∈ X

with: H(X) entropy;

p(x) probability,

:= is the symbol for "equal by definition", used for the definition of a concept by equality with other known concepts.

Where the entropy H(X) of a message source represents the "average" information contained in each emitted message, which is the greater the less likely it was originally (assumed). As a consequence of this, a message that is taken for granted and shows a high probability of being emitted by the source actually contains little information, whereas an unexpected and unlikely message contains a large amount of information.

As a consequence of this, given an alphabet of N symbols, the entropy of the legal universe $\log_n$ (N) in t symbols are used with the same frequency, and one can define legal "alphabet efficiency" transmitting information about the typical fact, becomes maximum if or when all sy as the ratio between its entropy and the maximum possible entropy found for an alphabet of N symbols:

$$H\left(X\right) := -\sum p\left(x\right)\log_2 p\left(x\right)/\log_2 N \qquad [2]$$

x ∈ X

Thus, in order to compress files without losing information, it is necessary to use an efficient alphabet. Furthermore, an examination of a compressed file with a text or hexadecimal editor reveals the significant randomness of the bytes present, which provides an opportunity to enhance the efficiency of the encoding process. Using, then, the Huffman encoding[82] and the arithmetic encoding[83], they must estimate the probability with which the symbols of the previous encoding occur in order to improve it. Information is measured in bits, which

py H reaches its maximum value when p(i) is equal to 1/r (where r is the total number of states). This allows for the definition of entropy to be accurately defined and represents the only possible definition. This is in accordance with the principles set forth by Claude Shannon in his seminal work, A Mathematical Theory of Communication.

79. It must fulfil three conditions: if A(k) has probability p(k)=0 of occurrence, then H(p(0), p(1)… p(k-1),0) = H(p(0), p(1)… p(k-1)); and given independent systems A and B there is subadditivity H(A,B)< H(A)+H(B).

80. In contrast to Shannon's approach, which considered the amount of information exclusively in probabilistic terms, whereby a discrete information source is represented as a stochastic process generating characters from a finite alphabet at each temporal instant, Shannon did not deal with semantic content.

81. Shannon 1948, pp. 379-423 and pp. 623-656; Shannon showed how a "random source of information cannot be represented with a number of bits=0.69315 nat [Ed: unit of measurement introduced by Shannon] lower than its entropy, i.e., its average self-information" This result was already implicit in John von Neumann's statistical definition of entropy, who, apostrophised on the subject by Shannon, did not consider it worthy of attention.

82. Huffman coding uses a specific method to choose the representation of each symbol, such as a code without prefixes, i.e., in which no binary string of any symbol is prefixed to the binary string of any other symbol, expressing the most frequent character in the shortest possible way.

83. Arithmetic coding is a compression technique without the loss of information. In computer science, data is represented as a fixed set of bits, for example, characters are often represented with eight bits. Since some symbols with arithmetic coding assume to appear more frequently than others, it assigns variable length codes to the symbols in order to minimise the total number of bits to be transmitted.

are defined as the uncertainty of an event occurring with probability ½. Alternatively, bits can be considered as the information that is obtainable by knowing the outcome of that event. As previously stated, entropy is employed to quantify the information embedded in a message. It was established that the entropy H(X) of a discrete random variable X with probability distribution p(x) represents the degree of uncertainty, or information, associated with the value of X.

Another measure of fundamental importance in information theory is the mutual information between two random variables X and Y, jointly defined as:

$$M(\mathrm{X},\mathrm{Y}) = \sum p(\mathrm{x},\mathrm{y}) \log_2 \frac{p(\mathrm{x},\mathrm{y})}{\mathrm{p}(\mathrm{x})\mathrm{p}(\mathrm{y})} \qquad [3]$$

where p(x,y) represents the joint probability distribution of X and Y, while p(x) and p(y) are the marginal probability distributions of the two variables, respectively. Mutual information informs us how much Y's knowledge reduces X's uncertainty; thus, it quantifies the "mutual" information, i.e., that shared by X and Y. In fact, we can also write:

$$M(\mathrm{X},\mathrm{Y}) = H(X) - H(\mathrm{X}|\mathrm{Y}) \qquad [4]$$

where H(X|Y) *is the* conditional entropy of X given Y, i.e:

$$H\left(\mathrm{X}|\mathrm{Y}\right) = -\sum\sum p\left(\mathrm{x},\mathrm{y}\right) \log_2 p\left(\mathrm{x}|\mathrm{y}\right) \qquad [5]$$

Mutual information can be regarded as a special case of the relative entropy D(p//q), defined:

$$M\left(\mathrm{X},\mathrm{Y}\right) = \sum p\left(\mathrm{x},\mathrm{y}\right) \log_2 p(\mathrm{x},\mathrm{y})/\mathrm{p}(\mathrm{x})\mathrm{p}(\mathrm{y}) \qquad [6]$$

where q(x) is an arbitrary probability distribution on X; In fact, it results:

$$I(\mathrm{X},\mathrm{Y}) = D(p(\mathrm{x},\mathrm{y})//p(x)p(y)) \qquad [7]$$

The relative entropy I(X,Y) is interpreted as the "distance" D (even if it is actually not) between the distributions p(x) and q(x), and while it is always non-negative (and is equal to o if and only if p = q), it is not symmetrical and does not respect the triangular inequality[84].

It has been shown in several studies[85] that an indicator of semantic relevance is given by the unevenness of the "occurrence"[86] profile of a word in a text: in fact, the presence of a word only in certain areas or domains of a (sentence) text means that it is linked to and represents a particular context or section.

Using Montemurro and Zanette's M-Z algorithm[87], based on this assumption, we aim to quantify the information contribution that each word adds to those contexts in which it appears: this index is represented by the difference between Shannon's mutual information assessed on the text (i.e., between the words of the sentence text and the contexts into which it is subdivided) and on a randomised version of the same, obtained by randomly mixing[88] all its words; in other words, it measures how far each of the words deviates from having a homogeneous occurrence profile.

Let us now subdivide the (sentence) text into contiguous sections of equal length: experimentally[89] we know that there exists a particular length that maximises the value of the index (and therefore also maximises the information), and that this maximum (global or absolute) is represented as unique (or extremal); this length varies according to the genre of writing (and, in the extended case, of the linguistic form used in the text) and is typically quantified around a thousand words.

We now derive the explicit writing of the information index.

84. In mathematics, the triangular inequality states that, in a triangle, the sum of the lengths of two sides is greater than the length of the third, in Ferrarese 2017, p. 41.

85. Montemurro 2014, pp. 5-16.

86. In corpus linguistics, occurrences are defined as the absolute frequency of a term in a given text, the presence of a word within the text of a paragraph, document, or book. The term is derived from the English word "occurrence".

87. Montemurro 2014; Montemurro 2010, pp. 135-153; Montemurro 2009, pp. 165-169.

88. For example, by means of the text randomiser compiler by Miniwebtool.com.

89. Montemurro 2009.

Consider a text consisting of N words, using a vocabulary of *K* different words, and a partition *P* of the text divided into intervals $A_1, \ldots, A_P$ of equal length (length is measured in number of words).

Let ω now be a word that appears n times in the text and n_j times in the interval A_j; we then define the conditional probability of encountering the word ω in the interval A_j, as:

$$\rho(\omega \Big| A_j) = \frac{n_j}{S} \qquad [8]$$

Then, the probability of finding the word ω throughout the text is:

$$\frac{n}{N} = p(\omega) = \sum_{j=1}^{P} p(\omega \Big| A_j) p(A_j) \quad \text{where } p(A_j) = \frac{1}{P}, \forall j \qquad [9]$$

We can now use Bayes' rule[90] and calculate the probability $p(A_j|\omega)$; we obtain:

$$p(A_j \Big| \omega) = \frac{p(\omega|A_j)p(A_j)}{p(\omega)} = \frac{n_j}{n} \qquad [10]$$

This indicates the probability of its occurrence within the *j-th* interval, given that it is present in the word *ω*.

Use these quantities to calculate the Shannon mutual information between text sections and word distribution, as follows:

$$M(\mathrm{P}, \Omega) = \sum_{A_j}^{\omega} p(A_j,\omega) \log_2 \frac{p(A_j,\omega)}{p(A_j)p(\omega)} \qquad [11]$$

One must now subtract, from this quantity, the mutual information obtained in a generic randomised text as a measure of the informational contribution of words understood as the tendency of words to distribute themselves unevenly throughout the text.

Let, then: $< \tilde{M} (A_j, \Omega) >$ the mutual "average information" between all possible permutations[91] of the text; the information index is defined as:

$$\Delta\mathrm{I}(\mathrm{P},\Omega) := M(\mathrm{P}, \Omega) - < \tilde{M}(\mathrm{P}, \Omega) > \qquad [12]$$

We observe that if we denote by $\tilde{p}(A_j|\omega)$, $\tilde{p}(\omega)$ and $\tilde{p}(A_j)$ the probabilities calculated on the randomised text and note that $\tilde{p}(A_j) = p(A_j)$ and $\tilde{p}(\omega) = p(\omega)$, the measure [12] can be written in terms of a difference of entropies calculated on the sentence text and its randomised version, respectively:

$$\Delta\mathrm{I}(\mathrm{P},\Omega) := M(\mathrm{P}, \Omega) - < \tilde{M}(\mathrm{P}, \Omega) > = \qquad [13]$$

$$= H(P) - H(\mathrm{P}|\Omega) - (< \tilde{H}(P) > - < \tilde{H}(\mathrm{P}|\Omega) >) = < \tilde{H}(\mathrm{P}|\Omega) > - H(\mathrm{P}|\Omega) = [14]$$

$$= \sum_{\omega=1}^{K} p(\omega) \sum_{j=1}^{\mathrm{P}} [p(A_j|\omega) \log_2 p(A_j|\omega) - < \tilde{p}(A_j|\omega) \log_2 \tilde{p}(A_j|\omega) >] \qquad [15]$$

$$= \sum_{\omega=1}^{K} p(\omega) \sum_{j=1}^{P} [p(A_j|\omega) \log_2 p(A_j|\omega) - < \tilde{p}(A_j|\omega) \log_2 \tilde{p}(A_j|\omega) > \qquad [16]$$

We derive the explicit writing of $< \tilde{H}(P|\omega) >$ on a randomised text divided into P parts of equal length, with ω word occurring n times in the text and n_j times in the interval A_j, obtaining:

$$= \sum_{\omega=1}^{K} p(\omega\ ) \left[< \tilde{H}(\mathrm{P}|\omega) > \mathrm{nbsp;} - H(\mathrm{P}|\omega) \right] \tilde{H}(\mathrm{P}|\omega) = -\sum_{j=1}^{P} \frac{n_j}{n} \log_2 \frac{n_j}{n} \qquad [17]$$

So, the average entropy over all possible random realisations of the text is:

$$< \tilde{H}(P|\omega) > = - \sum_{\substack{m_1+\ldots+m_P=n, \\ m_j \leq \frac{N}{P} \forall j}} \left[p(m_1, \ldots, m_P) \sum_{j=1}^{P} \frac{m_j}{n} \log_2 \frac{m_j}{n} \right] \qquad [18]$$

where $p(m_1, \ldots, m_P)$ is the probability of finding mj occurrences of *ω* in part *j*. Breaking down the expression [18] with respect to each of the P terms of the second sum, we obtain:

$$= -P \sum_{m_1=1}^{min\{n,\frac{N}{P}\}} \sum_{m_2+\ldots+m_P=n-m_1} p(m_1, \ldots, m_n) \frac{m_1}{n} \log_2 \frac{m_1}{n} = = -P \sum_{m_1=1}^{min\{n,\frac{N}{P}\}} p(m_1) \frac{m_1}{n} \log_2 \frac{m_1}{n} \qquad [19]$$

90. Bayes' rule links the inequalities of event A1 to event A2, before and after their conditioning to event B1. The relationship is expressed in terms of the Bayes factor, Λ. Bayes' rule is derived from and is closely related to Bayes' theorem.

91. In mathematics, a permutation is defined as an exchange of the order of a sequence of elements, which may be any, with the objective of finding the number of all permutations (i.e., all sequences with order) that can be formed given a certain number, n, of elements.

$$-\sum_{\substack{m_1+\ldots+m_P=n,\\ m_j\leq\frac{N}{P}\forall j}}\left[p(m_1,\ldots,m_P)\frac{m_1}{n}\log_2\frac{m_1}{n}\right]-\ldots-\sum_{\substack{m_1+\ldots+m_P=n,\\ m_j\leq\frac{N}{P}\forall j}}\left[p(m_1,\ldots,m_P)\frac{m_P}{n}\log_2\frac{m_P}{n}\right]= \quad [20]$$

To sum up, we can write the average entropy using the following formula:

$$<\tilde{H}(P|\omega)>=-P\sum_{m=1}^{min\{n,N/P\}}p(m)\frac{m}{n}\log_2\frac{m}{n} \quad [21]$$

where *p(m)* is the probability of finding the word ω exactly m times in one of the intervals A_j, or:

$$p(m)=\frac{\binom{n}{m}\binom{N-n}{N/P-m}}{\binom{N}{N/P}} \quad [22]$$

In order to test an M-Z algorithm in an entropic environment, we extract the words with the highest information content (*keywords*) from our judgment texts broken down by legal institutions, comparing these results with those obtained on a lemmatised version[92] of our corpus of judgments: To lemmatise our judgment texts we make use of a probabilistic-heuristic grammar annotator that makes use of decision trees, such as Lexicool[93], available GNU-GPL on the web[94].

92. To lemmatise a text means to replace each word, token, with its lemma, i.e., its non-flexed form.

93. Lexicool is a software available under the GPL licence that makes it possible to analyse a text and obtain grammatical analysis (tagging) and lemmatisation of individual words. "There are two advantages to lemmatisation and tagging of text: the first, due to lemmatisation, is the optimisation of the databases used. In these databases, only those lemmas will be present to which the forms in the text will be traced. Verbs will be present in the database conjugated in the infinitive and not in all the possible forms in which they can be conjugated; nouns will be present in the singular; adjectives and adverbs in English would theoretically not need to be lemmatised since they are indeclinable. This entails a considerable streamlining of the database and thus less memory space occupied by it, and a not inconsiderable increase in the speed of the software process and consequently of the analysis. The second advantage (deriving from tagging) consists in the fact that the software implemented will only be able to search the database on words belonging to certain grammatical categories, thus considerably reducing the number of queries to be made and consequently increasing the performance of the software. One might, for example, want to analyse only nouns or only adverbs. Tagging also makes it possible to divide the headwords in the database into different tables according to grammatical category and to search for each term in the analysed text in the appropriate table". Lexicool is 'the most complete and efficient research tool possible for linguists and especially for translators and interpreters. The site is managed by an international team of linguists and programmers based in France and headed by Sebastian Abbo, the site's founder. The team's main work consists of searching and classifying bilingual and/or multilingual dictionaries/glossaries in free access on the Internet. Each resource found is evaluated as objectively as possible according to presentation, user-friendliness, general usefulness and size (number of entries, number of languages). On this appreciation depends on the position of the dictionary/glossary in the search results. Currently, the directory has more than 8000 links and new resources been added every day. https://www.lexicool.com/text_analyzer.asp?IL=2.

94. In order to calibrate the model under study, we have considered a 'large corpus' composed of 34 texts of judgments of different monocratic rites (ordinary civil, labour, justice of the peace, civil appeal to justice of the peace, criminal) in their version in Italian only. This corpus has been indicated with the generic symbol Γ. It is, therefore, a non-parametric corpus of modest dimensions, yet one that enables the illustration of intriguing properties and the proposal of potential avenues for further reflection on the analysis methodology that can be adopted. In order to test the M-Z algorithm in an entropic environment, the words with the highest information content (keywords) are extracted from the sentence texts, with the results being compared with those obtained on a lemmatised version of the corpus. The process of lemmatisation involves replacing each word, token with its lemma, that is to say, with its non-flexed form. In order to lemmatise the sentence texts, a probabilistic-heuristic grammar annotator was employed which utilises decision trees, such as Lexicool, this tool is also primarily an annotator for parts of speech. Lexicool was employed for each original corpus text, designated as Γi, as well as for a lemmatised version of it, indicated as Λi. It was observed that the cardinality of the vocabulary in the texts with corpora Γ i and Λ i exhibited minimal change. The explanation can be found in the existence of blocked phraseologies in the sentential sphere. The literal 'applicable fact-law' method entails a linguistic standard of exposition for the adjudicator, both in the explanation and, even more so, in the writing of the motivation. The process of lemmatising a text has two principal benefits. Firstly, since lemmas encompass

We will observe that the cardinality[95] of the vocabulary in texts with corpora Γ i and Λ i hardly changes at all.

The current explanation can be attributed to the presence of obstructed legal phraseologies in the sentence, namely. The adjudicating operator must employ a linguistic standard of exposition when applying the literal applicable fact-law method. This standard should be used in the drafting of the motivation, which is a bound literal technique, rather than in the explanation of the sentence, which is free technique. Article 12 of the Italian "Preleggi" [trad. Pre-Laws] mandates that the law must not be given any meaning other than what is expressed by the proper meaning of the words and the intention of the legislature.

If a dispute cannot be decided by a precise provision, regard shall be had to the provisions regulating similar cases or similar matters; if the case still remains doubtful, it shall be decided according to the general principles of the legal system of the state. As is well known, a part of speech depends not only on the word itself, but also on the context: thus, simply associating each word with

entire classes of inflections, the redundancies inherent to the legal vocabulary are effectively eliminated. Secondly, it reduces the sparsity of data that is always present in the study of texts in sectorial natural languages, such as legal. The words are ordered in a decreasing sense with respect to frequency, which decreases with the trend of a cardinality of exponent ~ -1 (seen Zipf's law). Finally, the process of lemmatisation results in a reduction in the cardinality of the vocabulary, which in turn leads to an increase in the average word frequency. This is achieved without any loss of comprehensibility. The lemmatised text could generally rely on the informative contributions of a smaller number of words, but the total quantity of information conveyed is the same as that obtained from the original text. This indicates that the information conveyed by the lemmas is redistributed over their inflected forms. During the experimental investigation of merit sentences, it was observed that the keyword extraction process applied to sentence texts may yield results that are influenced by the presence of pronouns, prepositions, and verbs. As nouns are the category that gathers together all the semantic content of a sentential text, establishing its subjects and objects and limiting its legal themes, the extraction was carried out with the cleaning of spurious lemmatised terms. The Lexicool textual machine was employed as a part-of-speech analyser to facilitate the sentential pre-analysis procedure, which was then applied to the M-Z algorithm in an entropic environment for the purpose of assessing a causal impact. In this context, the sentential POS-tagger, which is pre-trained by Lexicool, was utilised to produce tagged output given an input corpus.

95. "In set theory, cardinality, or the number or power of a finite set, refers to the number of its elements: it is indicated by the symbols A, #(A) or card(A). The definition provides an abstract definition and a generalization of the concept of natural number that is also valid for infinite sets. The definition follows the following steps: • Two sets A and B are said to be 'equicardinal' or equipotent or even 'equinumerous' if a one-to-one correspondence can be established between their elements, that is, if each element of A can be associated with one and only one element of B, and vice versa. • It is noted that equicardinality is an equivalence relation (that in reality it only enjoys the properties that characterize equivalence relations) but in axiomatic set theory it is not an equivalence relation, due to the fact that the set of all sets equipotent to an assigned set A is not a set, but a proper class. Therefore, two sets are said to have the same cardinality or the same power if they are equicardinal". Halmos 1974.

its morphosyntactic category of highest probability is an inefficient way of POS-tagging[96-97].

To this extent, Markovian selection[98] appears efficient in literary contexts, but not with the constraint of the language of law, which establishes fixed forms for associating fact and law through a literal-judicial interpretation given by the law itself[99].

Legal sectorial linguistics systems exhibit "intermittent" behaviour, i.e., they alternate long periods of lexical inactivity with phases of hyperkinesis: for instance, in legal texts it is possible to discern a differentiated intermittency for $P(\tau)$ partitions (i.e., $P(\tau)$ distribution signals) in the occurrence profiles of law-specific terms. Thus, the rhythm of the legal term follows the fixity and mobility of the occurrence profiles.

If, in general, a binary string is constructed to visualise this phenomenon, whose *i-th* element is presented as equal to 1 if the event under consideration occurs at time i and 0 otherwise, and in such a case, through a Poisson process, the pattern is presented as random and the probability of an event is independent of time; thus, the return time between two consecutive events, τ, follows an exponential distribution.

Consequently, the rhythm of the legal term is contingent upon the simultaneous presence of both fixity and mobility in the occurrence profiles.

If, in general, we wish to visualise this phenomenon, we may construct a binary string, wherein the *i-th* element is equal to 1 if the event in question occurs at time i and 0 otherwise. In this case, through a Poisson process, the pattern is presented as random. Consequently, the probability of an event is independent of time. Therefore, the return time between two consecutive events, τ, follows an exponential distribution. The term "burstiness" or "intermittency" is employed when the pattern in question is not random.

It is well known that part of the language depends not only on the word itself but also on the

96. *PoS tagging* (part-of-speech tagging) assigns a tag (a tag is defined as a keyword or term associated with information, which identifies and describes the object, making it possible to reclassify and search for information based on keywords) to each word in a *document/corpus*. The choice of *tagset* to be used depends on the language/application being used. The input is a string of words and a *tagset* to be used and the output is the association of the 'best' *tag* with each word. Several *tags* can be seen compatible with a word (ambiguity case), the task of a PoS tagger is to resolve ambiguities by choosing the most appropriate tag according to the context of the word. One of the main problems of a probabilistic method is that it cannot deal effectively with the problem of sparsity of data; in the case of language, due to Zipf's law, this problem is well present, and so if one has a corpus of limited size, the POS-tagger will not work well. One of the methods that can circumvent this problem is the Tree-tagger; it makes use of a corpus annotated by parts of speech to construct a decision tree, which allows for good estimates of transition probabilities. So, we want to determine the probability that a word has p.o.s. $\tau \in$ T, with T being the set of parts of speech; then we consider the set of trigrams $[\tau,\tau\text{-}1,\tau\text{-}2]$, where $\tau\text{-}1,\tau\text{-}2 \in$ T are the possible P.O.S. preceding τ, and we construct the decision tree by proceeding recursively through tests. For example, one test is to ask whether or not it is true that τ-1 is a lemma; we then set $\{\tau\text{-}1 = NN\}$ as the first node of the tree and divide the set of trigrams into those that verify the test, and those that do not (similarly, the tree is also divided into two subtrees). We then proceed recursively with further tests τ-1 and τ-2.

97. Schmid 1994.

98. Manning–Schütze 1999. Lecture notes by F. Tamburini (University of Bologna) on word-space models; Hidden Markov models (HMMs) are used in numerous applications in natural language processing, such as automatic speech recognition, POS-tagging and other pattern recognition. Essentially, these are Markov chains that are allowed to emit a 'symbol' each time a state is reached. Formally, let $V = \{v1, \ldots, vn\}$ be a set of symbols and S a finite or countable set of Markov chain states with transition matrix A and initial distribution Π. Then an HMM is a triple $\Lambda = (A,B,\Pi)$ where $(B)i,j$ is the probability of generating the symbol vj when the state si is reached, i.e., $(B)i,j = (P(y(t) = vj \,|x(t) = si \in S)$, with $y(t) \in V$ being the symbol generated at time t and $x(t) \in S$ being the hidden state at time t.

99. Article 65 of the Judicial Ordinance, in indicating the powers of the Court of Cassation, states that it 'ensures the exact observance and uniform interpretation of the law, the unity of the national objective law, and respect for the limits of the various jurisdictions'; id est: the supreme body appointed to interpret the law must ensure uniformity and unity of the national objective law, confirming that the law is objective, i.e., it must be certain in order to allow for its control'; cf. Betti 1948, p. 13.

context: therefore, simply associating each word with its most likely morphosyntactic category is an inefficient way of doing POS tagging. At this point, apart from the Markovian selection , , , , which is efficient in literary contexts, but not with the constraint of the language of law, which establishes fixed forms to associate fact and law through a literal-judicial interpretation given by the law itself, in order to tag correctly, we explicitly formulate the so-called "supervised learning" rules for tagging, unanimously accepted by the scientific community, such as:

- manually annotate a sample of data (training corpus);
- let the program extract generalisations from the annotated data;
- use a program that has been "trained" on annotated data to annotate new data.

Obviously, taggers will work best when used to tag corpora similar to the training corpus, i.e., taggers calibrated only for judgments on the merits will give maximum efficiency when used for judgments in general, rather than when also used to tag legal literature in general.

In keeping with this, the *burstiness* or intermittency variable is introduced, on the other hand, only when, and to the extent that, the pattern being represented is not random.

Therefore, an effective indicator is calculated that can measure this trend by means of a mathematical lemma:

Lemma 1. Let σ be$_\tau$ *and* μ be$_\tau$, respectively,

- the standard deviation and the mean of $P(\tau)$;
- then the coefficient of variation, defined as $\frac{\sigma_\tau}{\mu_\tau}$;
- means the deviation (departure) from a Poissonian signal.

Indeed, it takes on a value of +1 for a Poissonian signal tending to $+\infty$ and for signals of distribution $P(\tau)$ with infinite variance and finite mean. We prefer, however, an indicator that collects values within a finite interval, and, therefore, we define the *burstiness* index as:

$$B = \frac{\frac{\sigma_\tau}{\mu_\tau} - 1}{\frac{\sigma_\tau}{\mu_\tau} + 1} \qquad [23]$$

The B-index takes values in the limited open range (-1,1), and the signals with the greatest *burstiness*, i.e., intermittence, are those that are closest to the +1 value.

Since words in a text can assume intermittent behaviour, it has been experimentally observed that such words tend to be those of greater semantic relevance. So, we use the index B precisely to calculate the *burstiness* of a word ω in a text string $w_1, \ldots, w_n$; to do so, we transform the text string into a binary string by replacing w_i with 0 if $w_i \neq \omega$, and with 1 if $w_i = \omega$.

If, in this way, we compute $B(\omega)$ for each $\omega \in V$, as the vocabulary of the text string, occurring more than 1 time (=Freq.(ω) ≥1, in the text), we finally obtain a distribution of values for B in the limited open interval (-1,1), whose words with the highest value of B will be our *keywords* [Tab. 1].

Continuing with the evolution of our algorithms, *clustering* consists of grouping a set of word-data according to an established distance between them: in the context of the study of legal language, it is necessary to form clusters (groups) of tokens that share meanings or linguistic functions, or that are together by strict linguistic construction. In fact, the token-words of a text can be represented by vectors in an n-dimensional space called *word space*, and can, therefore, be compared and clustered according to their appropriate reciprocal distance, which will be calculated shortly [Fig. 1].

A *word space* is a model in which words are represented as vectors in an n-dimensional space[100], which we want to represent as a locus of (legal) word meanings; we construct *word spaces* consistently with the so-called "distributional semantics", which states: "Words with similar distributional properties have similar meanings"[101].

100. This theory proposes the paradigm according to which words are distributed in a space in which they are at a distance from each other proportional to their degree of similarity, so that according to the distributional hypothesis "two words are the more semantically similar, the more they tend to appear in the same linguistic context".

101. Eichinger 2017, pp. 1489-1492.

Correspondence between information and frequency of words, in sentence no. 65/2017 of 12 January 2017 of the Court of Verona, section 3, civil jurisdiction							
3-word combination	Frequencies	3-word combination	Frequencies	3-word combination	Frequencies	3-word combination	Frequencies
delle buste paga	12	adempimenti in materia	3	dipendenti un trattamento	3	12 del 1979	2
in materia di	6	ai suoi dipendenti	3	iscritti agli albi	3	1 comma 1	2
materia di lavoro	6	calcolo e stampa	3	nel caso di	3	1 della l	2
buste paga in	5	caso di specie	3	passata in giudicato	3	23-ott-07	2
attività di consulenza	4	circostanza non contestata	3	per sua natura	3	25 i 0013649	2
centri di elaborazione	4	consulente del lavoro	3	redazione delle buste	3	adempimenti di cui	2
compilazione delle buste	4	consulenti del lavoro	3	riservasse ai suoi	3	agli albi di	2
datore di lavoro	4	della legge n	3	soggetti iscritti agli	3	ai minimi retributivi	2
di elaborazione dati	4	di attività di	3	suoi dipendenti un	3	ai propri dipendenti	2
tanto dal ccnl	4	di cui al	3	tra le parti	3	albi di cui	2
un trattamento economico	4	di cui all'art	3	0013649 del 23	2	alla normativa vigente	2
16-gen-15	3	di lavoro previdenza	3	103 del 16	2	all'entrata in vigore	2
Average	Standard deviation	Sum of frequencies	B			al primo comma	2
3,16	2,494	158	-0,118			al risarcimento del	2

Tab. 1 — *Example of correspondence between information and word frequency (it)*

According to Manning[102], semantic similarity between two words is a function of the degree of similarity of their "linguistic environment", i.e., the degree to which the so-called "distributional hypotheses" co-occur – in similar contexts.

On this position Kilgariff argued: "Where word senses have a role to play in a scientific vocabulary, they are to be construed as abstractions over clusters of word usages"[103]. A distributional model realised by means of a "word-by-word" (*WxW*) *occurrence* matrix, in which the occurrences of each word are counted in a limited closed interval [-a, a], contains this type of relationship (an example of a paradigmatic relationship turns out to be that

102. Manning–Schütze 1999.

103. Kilgarriff 1997, pp. 91-113.

DyLan TextTools v2.1.9 guest | esci | guida | italiano | english

Testo da analizzare | Suddivisione in frasi | Suddivisione in token | Parti del discorso | Annotazione | Analisi globale della leggibilità | Proiezione della leggibilità sul testo

SID	TID	token	lemma	POS	F-POS	tratti morfo-sintattici	ID testa	tipo di dipendenza
1.	1.	-	-	F	FC	_	18	punc
	2.	I.	I.	S	SP	_	4	mod
	3.	D.	D.	S	SP	_	4	mod
	4.	s.n.c.	s.n.c.	S	S	num=n|gen=n	18	subj
	5.	di	di	E	E	_	4	comp
	6.	S.	S.	S	SP	_	7	mod
	7.	F.	F.	S	SP	_	5	prep
	8.	e	e	C	CC	_	7	con
	9.	G.	G.	S	SP	_	7	conj
	10.	,	,	F	FF	_	11	punc
	11.	per	per	E	E	_	9	comp
	12.	conto	conto	S	S	num=s|gen=m	11	prep
	13.	di	di	E	E	_	12	comp
	14.	C.	C.	S	SP	_	15	mod
	15.	P.	P.	S	SP	_	13	prep
	16.	,	,	F	FF	_	11	punc
	17.	si	si	P	PC	num=n|per=3|gen=n	18	clit
	18.	occupava	occupare	V	V	num=s|per=3|mod=i|ten=i	0	ROOT
	19.	di	di	E	E	_	18	arg
	20.	redigere	redigere	V	V	mod=f	19	prep
	21.	le	il	R	RD	num=p|gen=f	22	det
	22.	buste	busta	S	S	num=p|gen=f	20	obj
	23.	paga	paga	S	S	num=s|gen=f	22	mod

Fig. 1 — *Tokenisation in the decision n. 65/2017 of 12 January 2017 of the Court of Verona, section 3 civil jurisdiction. By Dylan analysis v.2.1.9. Simplification SID 1-23. Randomized vers.*

between the words "judge" and "justice"). On the other hand, a distributional pattern obtained by means of a "word-by-document" (WxD) matrix, i.e., one in which – given a corpus of documents – one counts the occurrences of each word in each document, contains this type of relationship (an example is the relationship linking "judgment" to "order"). We establish, for the occurrence patterns of the extractable keywords, the metrics to be applied to the clustering algorithms, in order to identify the presence and intensity of the relationships existing between these words.

The (main) metric for calculating *word spaces* in linguistics is that determined by the "cosine distance" represented as follows:

$$d(x,y) = 1 - \frac{|xy|}{xy} = 1 - \cos\theta_{x,y} \quad [24]$$

Whenever we do clustering, therefore, we always adopt this distance. Furthermore, we only experiment on legal syntagmatic relations, using only WxD-type matrices.

One of the earliest approaches to the representation of word meaning in the NLP, which is still given as being little used due to the exact (and time-consuming in terms of usable computer processes) calculation of occurrences rather than the statistical approach based on the probability

of finding occurrences in the corpus, or through statistical averages, is the use of the co-occurrence matrix between words in the corpus, based on a window of ±*m* adjacent words: the "Word embeddings with Co-occurrences and SVD"[104], is the method that exactly expresses the occurrences in a matrix function according to distance-cosine and is legally acceptable as it responds with deterministic and not inferential probabilistic exactness, to Article 12 of the Preleggi. This symmetrical matrix, in essence, counts how many times a given word appears in the window of another within the corpus[105]. The concept behind this construction is that words with similar meanings should have similar usage within the corpus, with similarity reflected in the corresponding row x column of the matrix. We assume a corpus consisting of 3 simple sentences with a window of ±1 words, without taking punctuation into account, and we also include the <BEGIN> and <END> markers of the sentences in the count as follows:

<START> I purchased <END>
<BEGIN> I am the owner <END>
<START> I want to sell <END>

Iterating over all the words in the corpus, we obtain a co-occurrence matrix by counting the words that appear in the respective window [Tab. 2].

We immediately realise that the management of such a matrix, on a real corpus relying on a dictionary of at least 50k-100k words, becomes extremely large and difficult to manage. Moreover, we are faced with an extremely sparse matrix, since relatively "few" words will appear in the window of a given word, leaving us with a matrix composed largely of zeros. In order to make this model practically usable, it is therefore necessary to reduce the dimensionality of the vectors associated with each word, trying to lose as little information as possible. To this end, we use the singular value decomposition (SVD), which allows us in its reduced form to decompose a matrix in the form $A=UDV^T$, where:

104. Another approach used in the field of Natural Language Processing derived from the 2013 paper 'Efficient Estimation of Word Representations in Vector Space' (Mikolov, Corrado, Chen, Dean) is the Word2vec which are trainable models for distributed word representation: by proposing a system that can be trained iteratively on a corpus of documents, capable of learning the meaning of words through word embeddings of a fixed size, one should overcome the problems of dictionary extension. Compared to the co-occurrence matrix, it overcomes the concept of the preliminary calculation of co-occurrences via a $|V|\times|V|$ matrix and its subsequent reworking via SVD, which is cumbersome on extended datasets and dictionaries that may well exceed 100k-1M terms. *Word2vec* models are known as: CBOW (*Continuos Bag Of Words*) model that works on the averages of *word embeddings*; the *Skip-Gram* model that works on similarity and probability distribution of the generated context; the *Negative Sampling* model, consists of an approximation by sampling a set of *word embeddings* extracted according to the frequency Pn (w) of the relevant words in the corpus; the Hierarchical softmax model, involves replacing the entire output layer, including the U matrix, with a binary tree whose leaves are the words of the dictionary and each node of the graph (not a leaf) is associated to a word embedding that the model will learn. A fundamental property of the *Hierarchical softmax* is that each node is guaranteed to normalise the probability.

105. Vagueness is a characteristic feature of the lexicon of natural languages and of the legal lexicon, so special attention is paid to semantic nuances, both in a hermeneutic and in a pragmatic key. The corpus studied distinguishes, in particular in the argumentative part of the sentences, for example, between intent and gros "negligence", where "the subjective element of intent is present when the subject has voluntarily taken advantage of himself" and "gross negligence is present when the subject has acted with obvious carelessness, recklessness and incompetence", with serious disobedience to the law, or even when the behaviour is carried out with "an indisputable disregard of elementary obligation". On the other hand, the vagueness of the language of the law is due to the use of abstract terms that represent concepts of social value and imply evaluations of different "moral situations". Examples are: "diligence", "omission", "good faith", "good morals", all of which require clarification and contextualisation: 'It is thus possible to identify the violation of the canons of loyalty and protection inherent in the principle of good faith, which governs the execution of contractual relationships, including those of employment, pursuant to art. 1375 of the Civil Code, as well as the breach of the duty of care established by Art. 1176 of the Civil Code'.

	<START>	Me	I have	They are	I want	Purchased	Owner	Sell	<END>
<START>	0	3	0	0	0	0	0	0	0
Me	3	0	1	1	1	0	0	0	0
I have	0	1	0	0	0	1	0	0	0
They are	0	1	0	0	0	0	1	0	0
I want	0	1	0	0	0	0	0	1	0
Purchased	0	0	1	0	0	0	0	0	1
Owner	0	0	0	1	0	0	0	0	1
Sell	0	0	0	0	1	0	0	0	1
<END>	0	0	0	0	0	1	1	1	0

Tab. 2 — *Co-occurrence matrix e.g.*

– $A \in R^{n \times d}$ is the starting matrix of rank r,
– $D \in R^{r \times r}$ is a diagonal matrix, on which the singular values of A are placed, arranged on the diagonal in descending order $\sigma 1 \geq \sigma 2 \geq \ldots \geq \sigma r$;
– $U \in R^{n \times r}$ is an orthogonal matrix ($UU^T=I$), whose columns form an orthonormal basis for the space generated by the columns of A;
– $V \in R^{d \times r}$ is an orthogonal matrix ($VV^T=I$), whose columns form an orthonormal basis for the space generated by the rows of A.

At this point we can choose a new reduced dimension k<r for our vectors and consider the submatrix $U1_{:n,1:k}$ of dimension n×k as our new word *embedding* – thus truncating the dimensions *r* in the various matrices of the decomposition to *k*. In this way it can be shown that the new *embedding* captures, however, a relevant part of the variance of the embedding. $\frac{\sum_{i=1}^{k} \sigma_i}{\sum_{j=1}^{r} \sigma_i}$ relevant part of the variance *of the* original *embedding*.

In this way we are able to go from vectors (*word embeddings*) of tens of thousands of components, to vectors of a hundred or so components, retaining much of the encoded information and allowing us to work with manageable vectors to perform comparisons, similarities and other linear operations normally performed on word *embeddings*. Although this model apparently has limitations due to the high dimensionality of the starting matrix and its sparsity, which can be partially resolved through SVD, it has the advantage of maintaining efficiency and reliability in the presence of a codified and rigid language such as the legal language of judgement.

However, SVD decomposition requires quadratic time, but, above all, one must consider the problem of adding new words in the *corpus*, which entails modifying the entire co-occurrence matrix. Furthermore, there is an issue of imbalance between the frequencies of common and uncommon words, which often requires corrections and/or the elimination of the most common words that carry little meaning (e.g.: articles, conjunctions, etc.). Indeed, for our purposes, the representation of the pattern through *keywords* alone excludes "spurious" syntactic elements.

A final discussion deserves the choice of the judgement sample to construct the algorithmic protocol capable of generating judgements autonomously, as a virtual machine, a clone of the real judge and its direct emanation.

If the *keywords* taken from the judge's databases of previous judgments are loaded as input data, broken down by institute and case, and processed according to the illustrated protocol, the output is a written judgement including the operative part, exactly clones of what the judge could have produced, due to his cycle of mental habit and within the framework of the laws and codes. The advantage is obvious: the multiplication of the "human" judge into a judging "humanoid" machine, subject to the same laws as the "human", as an expression of its own will, since it can be tutored in due final control.

Obviously, the greater the size of the statistical universe under consideration, the more reliable the decision-making outcome and the lower the probability of error. However, it should be noted that the *MZ* algorithm of entropy reduction, which is applied to the text's syntropy at the outset, is the only truly statistical element that exists. Nonetheless, this does not invalidate the tagging of the keywords, which are the only elements required for the final processing.

Analyzing the entire set of judgments provides the only way to obtain an output free from statistical errors. This can always be achieved through the use of probabilistic sampling, which maintains a constant fit at Chi-square=0, with events-sentence distributed poissonically.

It is important to always explain technical abbreviations when first used. The probability distribution may be approximated with a Gaussian distribution when the number of events is sufficiently large (with mean square deviation equal to the square root of the mean number of events-sentence) or by utilizing maximum likelihood, reasoned-choice or other non-probabilistic methodologies.

6. *Keywords* as lemmas for robotic sentences

Generally speaking, lemmatising a text has two classes of benefits: firstly, since lemmas bring together whole classes of inflections, redundancies in the legal vocabulary used are eliminated. Secondly, it reduces the sparsity of data that is always present in the study of texts in sectorial natural languages, such as the legal language, and since the words are ordered in a decreasing sense with respect to frequency, the latter decreases with the trend of a well seen cardinality of exponent ~-1[106]. Lastly, lemmatising reduces the cardinality of the vocabulary and consequently increases the average frequency of words, without subtracting comprehensibility from its content. The lemmatised text could generally count on the informative contributions of a smaller number of words, but the sum of these quantities is the same as that obtained from the original text: thus, the information of the lemmas is redistributed over its inflected forms.

On the other hand, in keyword extraction performed on sentential texts, one can obtain a result compromised by the presence of pronouns, prepositions and verbs. As nouns gather all semantic content of a sentence, establishing subjects and objects, as well as rhythm and legal themes, extraction using the Lexicool textual machine as a part-of-speech analyzer is required. To arrive at a sentential pre-analysis, the M-Z algorithm must be applied in an entropic environment to assess causal impact. Spurious lemmatized terms are cleaned during extraction.

In this regard, we use the POS-tagger[107] of sentence, "pre-trained" taggers from Lexicool that, given an input corpus, produce tagged output. As is well known, a part of speech is not only dependent on the word itself, but also on the context: thus, simply associating each word with its most likely morphosyntactic category is an inefficient way of POS-tagging. Thus, apart from the Markovian selection[108], which is efficient in literary contexts, but not with the constraint of the language of law that establishes fixed forms to associate fact and law through a literal-judicial interpretation[109] given by

106. Montemurro–Zanette 2005.

107. PoS tagging (part-of-speech tagging) assigns a tag (a tag is defined as a keyword or term associated with information, which identifies and describes the object, making it possible to re-classify and search for information based on keywords) to each word in a document/corpus. The choice of tagset to be used depends on the language/application being used. The input is a string of words and a tagset to be used and the output is the association of the 'best' tag with each word. Several tags can be seen compatible with a word (ambiguity case), the task of a PoS tagger is to resolve ambiguities by choosing the most appropriate tag according to the context of the word.

108. Manning–Schütze 1999; Lecture notes by F. Tamburini (University of Bologna) on word-space models; Hidden Markov models (HMMs) are used in numerous applications in natural language processing, such as automatic speech recognition, POS-tagging and other pattern recognition. They are basically Markov chains that are allowed to emit a 'symbol' each time a state is reached. Formally.

109. According to a philosophical essay by Professor Luigi Vallauri Lombardi, who is Professor of Philosophy of Law at the University of Florence, there are no less than '144 different ways of interpreting a legal norm'. In general,

the law itself, in order to tag correctly, we explicitly formulate the so-called "supervised learning" rules unanimously recognised by the scientific community for tagging as:

- handwriting a sample of data (training corpus);
- let the programme extract generalisations from annotated data;
- using a programme "trained" on annotated data to annotate new data.

Obviously, taggers will work best when used to tag similar training corpora, i.e., taggers calibrated only to judgments on the merits will be most efficient for use in judgments in general, rather than when also used to tag law literature in general. Other non-Markovian tagging methods for approaching the study of judgments are: the Tree-taggerPOS tagging[110] the Hierarchical clustering (bottom-up)[111], the Kmeans[112], the EM[113].

For the choice of lemmas by means of a non-probabilistic – but qualitative – analysis, it is very efficient and convenient to engage the linguistic machine of *Opinion mining-Sentiment analysis* "Lexalytics" by Lexalytics, 48 North Pleasant St., Amherst, MA 01002, USA, useful both for defining

under the subjective aspect, interpretation is distinguished into doctrinal, judicial and authentic, while for the preordained rule that can be derived from the normative system, which is that dictated by Article 12, Paragraph I of the Dispositions of the Law in General: 'In applying the law, no other sense can be attributed to it than that made manifest by the proper meaning of the words according to their connection, and by the intention of the legislator'.

110. Schmid 1994; Montemurro–Zanette 2005, pp. 29-40. One of the main problems of a probabilistic method is that it fails to deal effectively with the problem of sparsity of data; in the case of language, due to Zipf's law this problem is well present, and so if you have a corpus of limitate size the POS-tagger will not work well; One of the methods that can circumvent this problem is the Tree-tagger; it makes use of a corpus annotated by parts of speech to construct a decision tree, which allows for good estimates of transition probabilities. So, we want to determine the probability that a word has p.o.s. $\tau \in T$, with T being the set of parts of speech; then we consider the set of trigrams $[\tau,\tau\text{-}1,\tau\text{-}2]$, where $\tau\text{-}1,\tau\text{-}2 \in T$ are the possible P.O.s. preceding τ, and we construct the decision tree by proceeding recursively through tests. For example, one test is to ask whether or not it is true that τ-1 is a lemma; then, we set $\{\tau\text{-}1 = NN\}$ as the first node of the tree and split the set of trigrams into those that verify the test, and those that do not (similarly, the tree is also split into two subtrees). We then proceed recursively with further tests τ-1 and τ-2.

111. Hierarchical algorithms have two main characteristics: they are strong (they form disjointed classes) and they recognise a structure, hierarchical, between the elements within a class. These characteristics are read graphically with a tree dendrogram, which has as its root the cluster formed by all elements and as its leaves the clusters formed by syn-groups of elements. The Bottom-Up Algorithm is an example of clustering. Starting with the individual og-jects (the leaves of the tree), the algorithm identifies the two most similar elements and combines them into a single cluster. This process is iterated until all elements belong to a single cluster.

112. The k-means is a non-hierarchical iterative clustering algorithm, i.e., it is based on the idea of finding, iteratively, an optimal partition of the dataset into a predetermined number of clusters (k). Generally, a random partition is considered as the first iteration. Moreover, k.means is a 'strong' algorithm, i.e., it assigns each vector xi one and only one cluster cl. Precisely: $cl = \{x_i \,|d(x_i, \lambda l) \leq d(x_i, \lambda_j), \forall j, 1 \leq j \leq k\}$, where: d is the distance used 'Euclidean' and $x_1, \ldots x_m$ are the vectors of the dataset, while $\lambda_1, \ldots, \lambda_k$ are the centroids of each cluster, redefined at each new iteration as the average of the vectors belonging to the cluster considered. The complexity is O(n) and convergence of the method occurs when the clusters calculated at the i + 1-ma iteration are the same as those calculated at the i-ma iteration (in this case, convergence at step i): convergence is however not taken for granted, as it may happen that the algorithm oscillates between two solutions; therefore, a check should be added in order to avoid the loop.

113. EM (Expectation-Maximisation) is an iterative, non-hierarchical, weak clustering algorithm: this means that it does not associate each vector with a single cluster of belonging in a deterministic manner but rather provides the probability of the vector to belong to each of the clusters. In theory, this idea is formalised by assuming the existence of unobservable data z_j, the z components of which$_{ji}$ assume value 1 if the j-th data belongs to the i-th cluster.

the entropic space of analysis, and for comparing sentences by expressing, through the parameters returned by the internal processing, a relative score. Lexalytics is useful both for defining the entropic space of analysis and for comparing the sentences by expressing, through the parameters returned by the internal processing, a score relative to the analysis of the unfolding and a score relative to the motivation of the decision; working with algorithms that isolate the extracted entities, *topics*, lexemic combinations, category readability, lexical profile, morpho-syntactic profile, tokens, lemmas, dependencies, parts of speech, sentence division and many other indices.

Pivotal to the sentimental or opinion theory is the scientific conviction of the authors mentioned in paragraph 5, that linguistic lexemes and habits given by priming and nudging influence the written verbal representation of sentences. While the legal practitioner's linguistic skills are utilized for the narrative unfolding in the judgement, their representation of the material fact is done so appropriately to the legal fact as in figures 4, 5, 6, 7.

In order to facilitate a more profound comprehension of the qualitative method by means of a lexical machine, it is first necessary to adopt any civil, criminal or even administrative judgment of the Italian legal system. In the present case, a civil-law judgment is to be adopted. As previously stated, the judge's mood is calculated in the section of the judgment entitled *Course of events*, which is reported by the judge using free-form linguistics [Fig. 2].

The subsequent step involves the calculation of the mood of the part of the judgment entitled *Reasons for the decision* [Fig. 3]. This section of the judgment is formulated in accordance with Article 12 of the Pre-Laws of the Italian legal system, which stipulates as follows: "In applying the law, no other meaning can be attributed to it than that made clear by the proper meaning of the words according to their connection and the intention of the legislature. In instances where a dispute cannot be resolved by a specific provision, consideration shall be given to the provisions governing analogous cases or matters. If the matter remains ambiguous, it shall be resolved in accordance with the general principles of the legal system of the State". Article 65 of the Italian Judicial Order stipulates the powers of the Court of Cassation. It states that the court "ensures the exact observance and uniform interpretation of the law, the unity of the national objective law, and respect for the limits of the various jurisdictions". In other words, the court's primary function is to provide a definitive interpretation of the law, ensuring uniformity and unity of the national objective law. This confirms the objective nature of the law, which must be certain to allow for its control. The result of literal interpretation is thus subject to logical interpretation, and although Art. 12 makes no mention of it, it is imposed by an intellectual requirement of the interpreter – who is a judge – who cannot disregard the general principle from which the law derives and the precise purpose it is intended to achieve. The former is the *ratio legis*; the latter, the *occasio legis*. The former illuminates the interpreter by elucidating the meaning of the rule, while the latter provides an explanation of the legislator's intention and the reasons that led to it. In the light of these elements, the content of the rule becomes clearer. It is noteworthy that the logical interpretation may contradict the literal or grammatical interpretation. In such cases, the interpreter must refrain from preferring the logical interpretation. The Supreme Court has explicitly stated that: "When the literal interpretation of a rule of law is sufficient to express a clear and unambiguous meaning, the interpreter must not resort to logical interpretation, especially if through that interpretation there is a tendency to alter the clearly expressed intention of the law". This principle was articulated by the Supreme Court in its 17 November 1993 ruling (Cass. Sez. Lav.). In accordance with the principle of *non liquet*, which precludes the consideration of alternatives or evasion of responsibility, the judge is obligated to determine the moment of motivation, when the arguments substantiating the interpretative choice made become unavoidable and compelling. Any judge is bound to provide the sole correct response to the question posed by the parties. This response must be given, unambiguous, and deemed appropriate by the judge. The motivation must endeavour to persuade that the judge could not have responded more effectively.

The process is further advanced through the calculation of the so-called 'Entities', that is to say, the keywords that evoke the 'sentiment' regarding the judge in accordance with the priming effect. The computational mood is then calculated from these individual entities [Fig. 4].

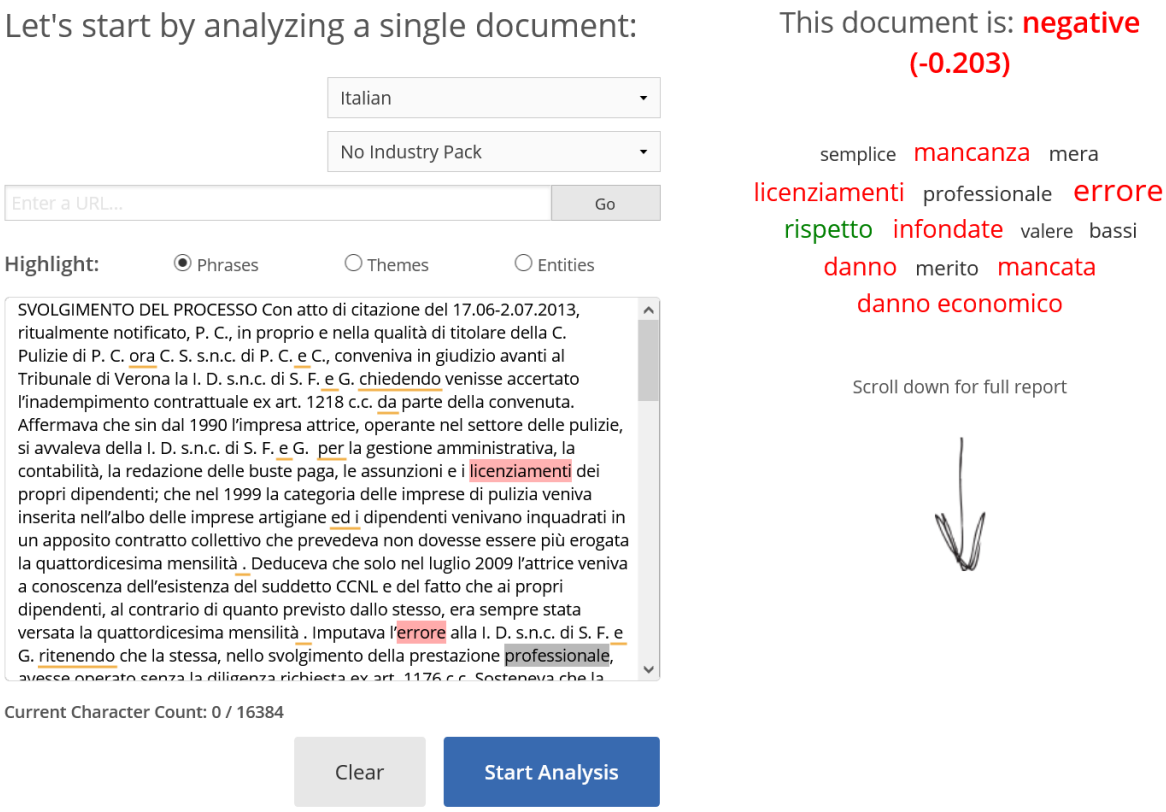

Fig. 2 — *Opinion mining analysis of decision no. 65/2017 of 12.01.2017 of the Court of Verona (Italy), section 3 civil jurisdiction. Course of events. By Lexalytics*

The "Items" associated with these entities are also calculated according to statistical evidence, i.e., with maximum correlation [Fig. 5].

To each item is assigned a sentiment according to its own linguistic dictionary. Each mood is thus weighed individually and, as a whole, is judged for the purpose of an ideological balance, producing expression of the judge's will.

This may include the use of technical terminology and objective language to maintain objectivity and clarity in the delivery of information. It is important to ensure the use of correct spelling and grammar while adhering to conventional academic structure and maintaining a balanced perspective. Additionally, precision is key in language choice to convey exact meaning appropriately.

A physical altercation with a troublesome superior is a relevant circumstance that may not necessarily be recognised as a legal fact, due to the expiration of the offence as a "non-execution of sentence". In the reasoning of the verdict, the judge rationalises their decision regarding the result of the legal fact, namely the intentional legal act, via a process of strict "interpretation".

The judge, who has full knowledge of the laws (*iura novit curia*) within the framework of the legal principle stemming from the bromcardo da *mihi factum, dabo tibi ius*, will act linguistically by means of established "routines" in ordering the judgement, acting on the same available verbal universe acquired over long focused legal studies, apprenticeships and professional updates followed, in the light of the economy of the process to be pursued.

For these reasons, the lemmatic analysis from which to draw capital *keywords* to be analysed and put in relation to each other to construct the structural equation with an explaining solution (the sentence), takes on a connotation more in keeping with reality if it breaks down the limits of the error given by the quantitative forecasting method, using a machine that assigns quality scores according to the perception of the social experience of the judge on the lemmatized term used. It has already been used for three decades to compose market analyses by means of a sociocultural target language.

Thus, when we speak of opinion mining-sentiment analysis in Lexalytics is nothing more than

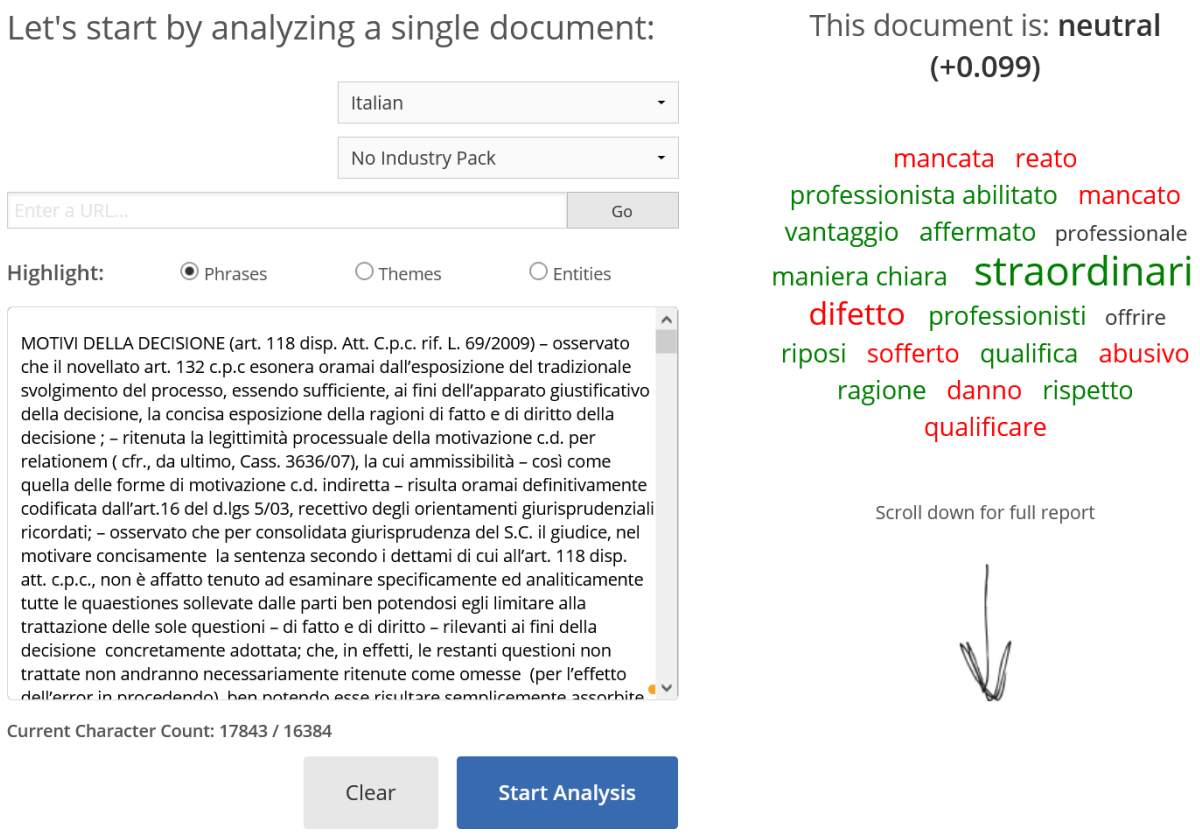

Fig. 3 — *Opinion mining analysis of decision no. 65/2017 of 12.01.2017 of the Court of Verona (Italy), Section 3 Civil Jurisdiction. Reasons for the decision. By Lexalytics*

the process of defining and categorising opinions in a given text as positive, negative or neutral. The three *machine learning* classification algorithms that are mainly used for *opinion mining* are:

– *Support Vector Machines (SVMs)*
– *Naive-Bayes*
– *Decision Trees*

Each has advantages and disadvantages; comparative studies have concluded that the *Naive-Bayes* classifier is the most accurate of the three.

There are also two main algorithms used within a lexicon-based approach:

– *Corpus*
– *Dictionary*

The *Naive-Bayes* classifier, which we prefer, is one of the three self-learning classification algorithms where each individual element is evaluated to determine the probability that the sum of these values leads to a predefined result: to better understand the concept, we can take as an example the offences of theft and embezzlement. If anyone takes possession of a thing, 'stealing' it from the person who owns it, in order to make a profit, he will most likely commit the crime of theft if he does not yet own the thing, embezzlement if he already owns it. Although these characteristics depend on each other or on the existence of the others, all these properties independently contribute to the likelihood of this legal act being sanctioned as theft.

Translating this into the sphere of motivations, we can state that a positive lemma may have a score of +1 while a negative lemma will have a score of -1. It is also possible to assign higher values to certain lemmas that may be more negative in terms of degree. In any case, if the final score of a mention is positive, then the mention is positive and vice versa for negative results. Let us take, as an example, a simple judging device and see how a Lexalytics computer would rank it if we assigned a score to the individual "terms" used, assuming we had already assigned a positive-negative score to a group of terms, such as:"exonerates" (positive/P) – "is not at all" (negative/N) – "relevant" (positive) – "motivate" (positive) – "concretely" (positive), "adopted"

Extracted entities	Associated themes	Evidence	Sentiment
G.	-	7	-3.21
Themes			**Sentiment**
ex art			+2.19
prestazione professionale			+2.19
diligenza richiesta			+2.19
giudizio avanti			-0.59
mera compilazione			-1.14
buste paga			-1.14
specifiche direttive			-1.14
chiedendo il rigetto			-1.49
domande attrici			-1.49
imputava l'errore			-2.45
Verona	+	5	-2.56
S. F.	+	5	-1.20
luglio 2009	+	3	-0.20

Fig. 4 — *Opinion mining analysis of the ruling n. 65/2017 of 12.01.2017 of the Court of Verona, Section 3 civil jurisdiction. Extracted entities. By Lexalytics*

(positive), "limit" (negative), "established" (positive), "jurisprudence" (neutral/NE).

Now let's take a hypothetical post of judgement that notes the mood (motivation/feeling) of the judging driver: "…having observed that (NE) according to the consolidated (P) jurisprudence (NE) of the S.C. the judge (NE), in motivating (P) concisely (P) the judgement (NE) according to (P) the dictates (NE) of art. 118 disp. att. (NE), it is not at all (N) obliged (N) to examine (N) specifically (NE) and analytically (NE) all (P) the quaestiones (P) raised (P) by the parties (NE), being able (P) to limit (N) himself (P) to the treatment (P) only of (N) questions (NE) – of fact (NE) and of law (NE)- relevant to (P) the decision (P) concretely (P) adopted (P)".

Each lexeme appears only once, and if we assign a "1" to each positive and negative value, then we can simply divide the positive and negative words by the amount of words (30) in the entire mention.

- Positive words: 13/30 = +0.43
- Negative words: 5/30 = +0.16
- Neutral words: 12/30 = +0, 40
- Tempest on mood: [P]0.43 – [N]0.16 = + 0.27
- Prevalent content (ideological drag) : P+N-NE = +0.19

Since the total of our mention is positive, we can say that the mood of the above-mentioned is positive. This is a fairly clear-cut case, because we did not encounter polarising words, the *keywords*, which could distort the result if a computer cannot work out which category the word belongs to. In the case illustrated, one can see an ideological drift given the positive translations of the data with respect to the neutral element.

Finally, the use of a lexical *mining* machine offers innumerable advantages over quantitative POS-tagging methods: 1) they assign points and frequencies on lexemes instead of just frequencies; b) they assign frequencies and positions in the corpus; c) they assign values socially deemed as positive and their negative opposite weighted. It is evident that the comparison of positive and negative values and their summation determines a result value that allows a *mood of the judgment* to be weighed, i.e., how much the judgment weighs the *sentiment*

70 themes

more info | api documentation

Extracted themes	Evidence	Sentiment
accertato l'inadempimento contrattuale ex art	7	-3.30
adeguare la gestione delle buste	7	-0.25
apposito contratto	7	-1.09
assegnati i termini	7	-3.17
assegnava i termini	7	-2.18
attività di consulenza	7	+2.27
atto di citazione	7	-1.15
bassi rispetto	7	-5.09
buste paga	7	-12.15
CCNL con mancanza	7	-5.09
chiedendo il rigetto	7	-9.38
chiedevano la concessione dei termini	7	-2.60
comparsa di costituzione	7	-1.70
comparse conclusionali	7	+0.15
confronti di un dipendente	7	-5.09
conseguente inapplicabilità	7	-10.89
contratto per iscritto	7	+1.39
danno economico	7	-5.09
danno ex art	7	-17.10
Deduceva l'inapplicabilità dell'art	7	-2.58
diligenza richiesta	7	+6.42

Fig. 5 — *Opinion mining analysis of the sentence n. 65/2017 of 12.01.2017 of the Court of Verona, Section 3 civil jurisdiction. Themes. By Lexalytics*

of the people who, through their representatives, formed the laws. The judgement thus becomes a thermometer of the social *mood* that also reveals any ideological dragging of the judgement against the legal provision of Article 12 of the Pre-Laws.

7. The *acceptance* of robotic sentences

The debate on robotic decision-making is an extraordinarily important topic that raises fundamental questions about the future of the legal system. This debate starts with the following question: is it possible to imagine a future in which judicial decisions are completely entrusted to robotic systems, based solely on the application of algorithms?

In this discussion, it is important to consider legal calculability and the value of precedent[114]. Legal calculability refers to the ability to precisely and computationally define legal rules and princi-

114. Carleo 2017, p. 193. On the first applications of artificial intelligence systems in the judicial sector, see also: Castelli–Piana 2018, p. 154 ff.; Livni 2017; Carleo 2019, p. 341.

ples that guide legal decisions. Precedent value, on the other hand, concerns the importance of past decisions in shaping law and creating legal precedents.

However, before embracing the idea of a fully automated justice system, we need to consider some fundamental issues. First, there is the ethical dilemma concerning the use of technology in justice. We must ask ourselves whether it is acceptable, in terms of legal education and the fundamental principles of the legal tradition, to entrust meaningful decisions to algorithmic systems. This raises concerns about the loss of humanity and discernment in decision-making, which are essential values for justice[115].

Furthermore, the issue of calculability and predictability of decisions raises questions about the very purpose of judicial decision-making. While the use of technology aims to improve the efficiency and predictability of decisions, we have to question whether this goal is compatible with the intrinsic purpose of justice, which is to assess and resolve disputes fairly and based on the specific facts of each case.

It is fascinating to observe how the idea of using a robot, based on the application of an algorithm, to issue judicial decisions elicits very varied reactions among jurists, oscillating between enthusiastic interest, concern and sometimes dismay. This debate epitomises the conflict between technological innovation and legal tradition, shedding light on essential questions for the future of the legal system[116].

It should be noted that, when assessing the efficiency of an economic system, two of the main indicators considered are the efficiency of the legislative and judicial system, and the duration of legal disputes. These are aspects that the jurist cannot ignore, since, as Riccardo Orestano states, "the jurist can never abstain or alienate himself from life and its knowledge"[117].

Enthusiasm for the idea of robotic decision-making is often fuelled by the promise of greater efficiency and timeliness in the resolution of legal disputes. The possibility of quick and objective answers to legal problems may seem tempting. However, this prospect also raises legitimate concerns about the loss of humanity in decision-making. The role of the judge is not only to apply the law mechanically but also to exercise discernment, sensitivity and understanding of the nuances of situations.

When we discuss the robotic decision, we are really entering a new era, a radical change in the paradigms of justice and law. In this context, IT tools stop being mere aids for communication, managing legal documents or searching for information. They take over the main role in decision-making in complex legal contexts. This concept has given rise to a new terminology: "robogiudians", a definition coined by Max Tegmark, a physicist at MIT[118].

The idea of "robot judges" raises fascinating and revolutionary prospects for the legal field. They could be thought of as highly specialised software capable of handling a wide range of legal cases in parallel, rather than serially as is often the case with human judges. This ability to work simultaneously on all pending cases could lead to a significant reduction in trial time and related costs, making the legal system more accessible and efficient for all[119].

Another aspect to consider is the prospect of "robot judges" with unlimited memory and learn-

115. See on the topic, Various Authors 2019, p. 1656 ff.; Rordorf 2018, p. 4 ff.

116. The relationship between techne and law is developed in the well-known dialogues by Irti–Severino 2000, p. 665, then collected in Irti–Severino 2001; in this regard, see also Severino 2013, p. 87, on the prevalence of technology 'destined to become, from means to ends… and, subordinating every force to itself, it establishes a hierarchy, recognises to every force what is due to them within that hierarchy, thus realising the form of justice to which society is destined to achieve'.

117. Orestano 1987, p. 335.

118. Robogiudists' are artificial intelligence systems designed to meticulously apply the same rigorous legal standards to every legal matter. They act tirelessly without falling victim to human error, such as bias, fatigue or lack of up-to-date legal knowledge. This perspective promises objectivity and consistency in the application of law, eliminating the variability that often characterises human decisions; Tegmark 2018, p. 143.

119. *Ivi*, p. 144.

ing capabilities. Unlike human judges, who may have limitations in understanding complex technical issues, these systems could successfully deal with a wide range of cases, from patent disputes to murders, due to their ability to constantly learn and adapt. This could help ensure greater uniformity and objectivity in legal decisions[120].

A critical aspect emphasised by proponents of robotic decision-making is the predictability of decisions. This recovery of "legal calculability" is considered an important value, as it promotes equal treatment of citizens. The idea is that "roboticists" apply laws and legal principles consistently, avoiding the subjective variations that can occur in human decisions. This would contribute to a fairer and more predictable legal environment for all.

Interestingly, these ideas are not entirely new. As early as 1969, the jurist Losano hypothesised that cybernetics could be a tool to promote equality by counteracting judicial creativity that can lead to inequalities and the skills of expert lawyers that may not be accessible to all[121].

The perspective of "robogiudists" offers a fascinating vision for the future of the legal system, with the possibility of greater efficiency, uniformity and predictability in decision-making. However, these ideas also raise important ethical, legal and social questions that require careful consideration and reflection as we approach this new era of justice.

8. The physiological limits of the human judge

In the period between the 1920s and the late 1930s, a current of legal thought known as "legal realism" emerged in the United States. This current represented a significant departure from the formal theory of law that had dominated the field until then. Legal realism vigorously opposed formalism, which limited legal reasoning to mere demonstrative logic.

One of the leading proponents of legal realism was Jerome Frank, whose 1930 work made an impressive critique of the formalist conception of jurisprudence. Frank argued that judges' decisions were not the result of rigorous logical reasoning, but rather of "intuitions" through which judges arrived at a final decision. These intuitions often preceded any attempt at justification or explanation. According to Frank, the determining factors in judicial decisions were psychological, moral, political and economic[122].

In this context, the legal norms cited in judgments were regarded as mere formal elements, often used to justify or legitimise decisions made on the basis of other considerations. Legal realism raised important questions about the very nature of legal decision-making and led to a critical review of previously dominant theories in the field of law.

Legal realism highlighted the inherent limits to the decision-making operation of judges, challenging the traditional idea that judgments were the result of a rigorous process of logical application of laws. This movement helped to "desacralise" the role of judges and their decisions, challenging the image of judgments as supreme manifestations of the magistrates' thought and methodological logic.

An aphorism emblematic of the realist perspective is the famous phrase "Justice is what the judge ate for breakfast" paraphrased in the title of an essay that appeared in the 1990s that fuelled this realist perspective and aroused lively interest in the legal debate[123]. This expression satirically condenses the realist view that judicial decisions were often influenced by subjective, personal or even random factors, rather than by a strict and impartial application of the law.

In an interesting study conducted by three researchers at Columbia University in collaboration with Tel Aviv University, the topic of rational decision-making in judges was addressed. The surprising results of this research seemed to confirm critics' concerns about rationality in the decision-making processes of judges[124].

120. *Ibidem*.

121. Losano 1969. Losano's further contributions on the subject are also important. In particular: Losano 1967, pp. 1589-1602; Losano 1966-1967, pp. 307-325; Losano 1971, p. 152 ss.; Losano 1978, pp. xii-xiv.

122. Frank 1930, p. 448.

123. Kozinski 1993, p. 993.

124. Danziger–Levav–Avnaim-Pesso 2011, pp. 6889-6892. For more on the subject, Marzocco 2018, p. 272.

In the study, the researchers closely examined the findings of no less than 1,110 sentences handed down by eight judges of two separate Israeli courts. These courts were responsible for deciding whether or not to grant freedom for good behaviour to prisoners held in the country's four largest prisons. In terms of our legal system, this judiciary would roughly correspond to the Surveillance Court.

The results of the survey revealed a surprising trend: the rate of granting parole requests decreased by 65% when decisions were made at the beginning of each work session or shortly after the morning coffee break or immediately after the lunch break. In other words, favourable sentences seemed to be concentrated at specific times of the judges' working day.

This study analysed the work of judges over a 10-month period. The results raised important questions about the rationality of judicial decisions and the effect of the time of day on their ability to make impartial decisions. In particular, they highlighted how external circumstances, such as fatigue or hunger, could significantly influence judges' decisions, raising important ethical and procedural questions in the judicial system.

In this study, each judge dealt with a significant amount of cases each working day, dealing with a range from 14 to 35. The research examined several variables, including the order in which the cases were presented (i.e., after how many prisoners their case was called), the time of day the cases were dealt with, the ethnic origin and background of the prisoners, as well as the type of offence they were convicted of.

During the course of the day, the judges regularly took two breaks, one for coffee and one for lunch, each with varying times and durations, and had three consecutive work sessions. This allowed the scholars to examine not only the effect of time on the judges' decision-making, but also the impact of the breaks on their decision-making ability.

The results of the survey revealed a surprising pattern: the tendency for prisoners to pass favourable sentences was much more pronounced at the beginning of each work session, but gradually declined as time passed until it became insignificant. However, this trend would reverse and return to its peak after coffee or lunch breaks. What was clear from this study was that factors completely unrelated to the legal issues dealt with significantly influenced the judges' decisions.

A simple interruption of work and the intake of a drink or food was enough to cause judges to treat often entirely similar cases differently. This phenomenon raised important questions about the consistency and impartiality of judicial decisions and underlined the extent to which environment and personal circumstances could influence the judges' decision-making process.

Understanding the results of this study required an analysis that went beyond the field of law, exploring the spheres of the psychobiology of the brain and the physiology of the human body. It was discovered that repetitive work, accompanied by the need to make similar decisions in an almost systematic manner, can gradually exhaust an individual's mental resources, impairing his or her ability to plan, adapt and evaluate actions efficiently. Routine tends to weaken so-called "executive functions" and can lead to conditioning in decision-making involving almost identical situations[125].

Mental fatigue may increase the decision-maker's propensity to simplify problems, prompting him/her to rely primarily on similar past experience. However, it is interesting to note that the ability to tackle problems in a more considered manner is restored, and mental fatigue is overcome, after a short break and an increase in blood glucose levels, which can be achieved through the consumption of drinks or food.

In other words, this study highlights how the judge's physical and psychological condition can influence judicial decisions in surprising ways. Mental fatigue and routine can lead to a more superficial approach to decision-making and a tendency to follow precedents without properly assessing the specific circumstances of each case. However, a break and an adequate supply of glucose can help restore mental clarity and the ability to make more considered decisions. These results highlight the importance of considering not only legal aspects, but also psychological and physiological ones in the context of judicial decision-making.

125. Eagleman 2016, p. 220. For more on the subject, Ekman 1999, p. 508; Ekman–Oster 1979, pp. 527-554; Fiandaca 2013, p. 408; Fuselli 2013, p. 256.

The results of this study highlight the importance of the judge's psychophysical condition even in decisions involving the responsibility of a defendant. The resting condition of the judge can, in fact, have a significant impact on the quality of decisions. A well-rested judge is more likely to make well-considered decisions than one who is tired and exhausted by the daily routine.

The researchers also examined the importance of the length of hearings and how much the time factor can influence the decision-making process. It turned out that the longer a hearing lasts, the greater the risk that a judge's mental fatigue negatively affects his or her propensity to make favourable rulings. This raises interesting questions about time management in judicial hearings and the need to consider the rest requirements of judges during proceedings that may extend over many sessions.

While there is a lack of specific empirical data to assess the effect of breaks, such as lunch breaks, in the context of long and complex hearings, one undeniable fact remains: factors outside the technical and legal issues can significantly influence the decision-making process, even when judges with established professional experience are involved.

9. Will there ever be a *just judge*?

Scholars identify a number of factors within the proceedings that can contribute to judicial errors[126]. Often, the error is attributed to a kind of "deviation" by the judge from the rational path outlined by epistemological rules. These rules aim to establish in concrete terms the relationship between probability and proof, using appropriate inference criteria such as the maxim of experience, statistical law or scientific law with varying degrees of empirical reliability.

However, it should be noted that judicial errors may result from a complex combination of factors, some of which may not be strictly related to epistemological rules. These factors may include emotional influences, mental fatigue, psychophysical conditions of the judge, factors external to the trial itself, or even the interpretation of evidence in complex and evolving contexts.

In addition, it is important to emphasise that miscarriages of justice are not only limited to wrong decisions in terms of the guilt or innocence of the defendant, but may also relate to the size of the sentence or other procedural issues. Therefore, the analysis of miscarriages of justice requires a thorough understanding of all these factors and the complex dynamics that can influence decision-making in the justice system.

The causes of miscarriages of justice can be attributed to a wide range of factors, which often include human behaviour, whether guilty or innocent, but also circumstances due to chance, misleading appearances or even outright fatalities. These factors can be divided into categories that include aspects related to the trial system, but also influences external to the trial itself.

One of the relevant factors is human behaviour. Errors may result from decisions of the protagonists involved in the trial, whether they act in good or bad faith. However, the causes of errors cannot always be attributed to individual responsibility, as there may also be situations where the innocence of a defendant has not been adequately recognised due to misleading or manipulated evidence or testimony.

In addition to causes related to human behaviour, there are factors that fall into the sphere of coincidences or false appearances. In some cases, mere chance can lead to miscarriages of justice, while in others, circumstances can create an illusion of guilt or innocence.

More, there are influences outside the process itself that can contribute to miscarriages of justice. The press, mass media and, more recently, the Internet and social media, can exert a strong influence on public opinion and, consequently, on the judicial process. Often, sensationalist narratives and the tendency to emphasise the emotional aspect of cases can distort the perception of reality.

Sociological research has shown how television, in particular, can exert a powerful suggestive force through images, significantly influencing opinion formation. This phenomenon can lead to a distorted reading of reality, in which the emotional aspect prevails over the rational evaluation of evidence.

Misperceptions or distorted perceptions pose a threat as they influence people's opinions, attitudes and behaviour. Thus, they can lead us to make decisions based on prejudices or misleading perceptions, influencing our attitudes and behaviour. It

126. Troisi 2011, p. 304; on this topic see also Imposimato 2009, p. 442.

is therefore crucial to be aware of these external influences and try to critically evaluate the information presented to us, especially when it comes to legal and judicial matters.

The phenomenon of the spectacularisation of trials has become an obvious reality with wide public resonance[127]. It is enough to think of court cases such as that of Perugia, linked to the murder of Meredith Kercher, which divided public opinion between those who believed in the innocence of the defendants and those who supported their guilt. Similarly, the trial of Annamaria Franzoni, accused of the murder of her little son, or the case of the death of Alberto Stasi's girlfriend, which saw the final conviction of the young defendant. The spectacularisation of trials has become increasingly invasive, often overstepping the boundaries of the legitimate exercise of the right to report news. This phenomenon has had a significant impact on the lives of those involved, creating an overlap of television broadcasts that, in some cases, seem to anticipate or even replace the judicial decision. During these broadcasts, witnesses and experts, often more or less qualified, are interviewed and "alternative truths" are proposed in order to increase the television audience. This approach can have a considerable impact on public opinion and can sometimes undermine the fact-finding process, which should take place in an impartial and rigorous manner within the appropriate court context[128].

Television broadcasts tend to arouse strong emotions in viewers, often influencing public perceptions of court cases. In particular, in trials before a jury of popular judges, there is a risk that these jurors, as television viewers, will be influenced by the emotional stirrings and suggestions in the broadcasts. This can be a problem, since the task of the jury is to reach an impartial decision based solely on the evidence and the law, without being influenced by outside influences. Therefore, it is important to carefully consider the impact of the spectacularisation of trials on public perception and the legal system as a whole.

The use of media in the trial represents a challenge for both the defendant and the justice system, and this issue is considered among the main causes of miscarriages of justice[129]. While in the real trial, the defendant enjoys the presumption of innocence, in the media trial, which is often characterised by a sensationalist narrative, the defendant is forced to defend himself against a potential justicialist drift[130].

Scholars tend to attribute most miscarriages of justice to the incorrectness or even falsity of the evidence presented. False testimony, a distorted perception of the facts by witnesses, or a lack of understanding by the judge of the basic principles of testimony can lead the judge to wrongly convict an innocent individual. In addition, a personal investigation conducted improperly, in violation of court rules or in an unprofessional manner, can lead to miscarriages of justice. Similarly, a confession obtained through coercion by investigators, especially on psychologically vulnerable individuals, may lead to wrongful conviction.

It is important to note that the media attention on a court case can amplify these problems, as it can influence public opinion and put pressure on the justice system to deliver a verdict quickly. Therefore, it is crucial to strike a balance between freedom of the press and the goal of ensuring fair and impartial trials, so that media use of the trial does not become a threat to justice itself.

Scientific evidence, although often regarded as a source of objective evidence, can also deviate from the truth. In such cases, it is experts, acting as expert witnesses or consultants, who can lead the judge to an erroneous conclusion in the case. This phenomenon can be observed in various legal systems, with the US experience providing significant examples.

Federico Stella, in particular, analysed the accusatory paradigm and the antagonistic structure of the criminal trial, noting that this has led experts to adopt a kind of "partisan culture". This culture leads experts not to separate facts from scientific opinions, opinions from conjecture, and questions

127. Amodio 2016, p. 274.

128. Kalb 2005, p. 239.

129. Troisi 2011, p. 304; on this topic see also Imposimato 2009, p. 442.

130. Paulesu 2008, p. 600.

of fact from value choices[131]. This phenomenon is often associated with the concept of pseudoscience or so-called "junk science", and has been widely examined by legal process scholars, especially in the United States"[132].

This may lead the judge to form an erroneous conviction, wrongly assuming that the elements provided by scientific evidence are subject to objective evaluation. In the presence of evidence based on scientific knowledge, the judge may erroneously withdraw from his evaluative function[133].

In fact, the role of the judge should be to carefully examine the margin of error present in any scientific method and the expert should be obliged to clarify the probability of error associated with the scientific model used. In this way, scientific evidence can be prevented from being distorted or misunderstood, ensuring a fair and impartial trial based on reliable scientific knowledge. The issue of judge subjectivism is a crucial aspect of the criminal trial, yet scholars in this field have often not given it the attention it deserves. In the past, questions have been raised about the judge's insufficient caution or experience in evaluating evidence, the difficulties in distinguishing between truthful and untruthful testimony, and the challenges associated with the statements of weak subjects, such as minors[134].

However, it is surprising to note that there has been relatively little reflection on the fact that the conclusive judgement of a trial is often based on intuition rather than strict logic. This statement was made as early as the beginning of the last century by scholars such as Altavilla[135]. To fully understand this dynamic, it is useful to consider the words of Calamandrei, who emphasised that, except in pathological cases, the judge is influenced by reasons not declared even to himself. These are unconscious sympathies or repulsions that intuitively guide him to select a legal solution from among many possible ones, a solution that reflects these hidden feelings[136]. These feelings may be triggered by the emotions aroused in the judge by the human case under discussion, and in this way may unconsciously condition his judgement.

This element of subjectivity is an important challenge to be faced in the legal system, as it underlines how complex it is to achieve a completely impartial decision. Few, like Piero Calamandrei, have written of the verdict, without mincing words, "that the motivation is nothing more than an expedient of formal hypocrisy, made almost, one might say, to give a logical disguise to a will born of quite different motives that may be arbitrariness and injustice"[137].

The idea that the justification of the judgment can serve primarily to validate a hypothesis already formed by the judge represents an intriguing and incisive perspective within the judicial system. This concept suggests that, in reality, the judge's decision-making process may be largely intuitive, with the justification following later to provide a retroactive rational justification.

Moreover, this insight sheds light on the understanding of judicial decision-making. Jerome Frank, one of the leading figures of legal realism, had clearly emphasised that judges are no different from other people and that irrational forces can play a significant role in their decisions. This represents a realistic and humane view of the judicial system, contrasting with the traditional idea of judges as purely rational and objective beings.

This view challenges the image of the judge as a being completely immune to emotional or irrational influences. On the contrary, it suggests that judges, like all individuals, can be influenced by emotional, personal or psychological factors that can significantly shape their decisions. Therefore, recognising this human dimension in judicial decision-making is crucial for a more complete and realistic understanding of the functioning of the legal system.

131. Stella 2001, p. 608.
132. Jasanoff 1995, p. 400.
133. Dominioni 2005, p. 372.
134. Pisapia 1989, pp. 165-178.
135. Golding 2001, p. 187.
136. Calamandrei 1965, p. 618.
137. Calamandrei 1954, p. 157.

Cappelletti's view that the real motivation for a judgment lies in the judge's feelings and emotional sphere emphasises the importance of subjective variables in judicial decision-making[138]. This perspective suggests that free conviction, which forms the basis of judicial evaluation, is intrinsically linked to a discretion that can result in personal intuitions, feelings, emotions and sometimes even ideological beliefs, personal values and subjective worldviews.

In other words, the judge's decision-making process cannot be separated from his or her personal experiences, emotional inclinations and personal convictions. This recognition challenges the idea that law is an exclusively rational and objective discipline, emphasising instead the human and subjective dimension that permeates the legal system.

The various regulatory strategies adopted in the various trial systems to limit the judge's discretion and regulate the use of evidence have often proven their insufficiency in preventing miscarriages of justice. This highlights the complexity of judicial decision-making and the difficulty of completely reducing subjectivity in the evaluation of evidence. Indeed, these challenges reinforce the importance of greater awareness of the human and emotional factors that can influence judicial decisions, as well as the need for constant improvement of methods and protocols to minimise judicial error.

The analysis of psychological phenomena such as instinct, intuition, subjectivity, emotions, feeling and bounded rationality is a fundamental approach to better understand judicial decision-making. While traditional trial-criminal doctrine tends to neglect these aspects, psycho-legal research and cognitive sciences have long recognised their essential role in judicial decision-making. It is important to emphasise that errors in judicial decision-making are not random, but often result from predictable patterns of thought operating under conditions of uncertainty. These errors can be difficult to anticipate and control, as they are ingrained in the common way of reasoning and decision-making.

In other words, the risk of making mistakes is present in any human activity involving the making of a judgement, and this is particularly true in the judicial context, where the consequences of decisions can be significant for the lives of the people involved.

10. Concluding reflections

In this context, it may be necessary to intervene in order to ensure the pseudonymisation or encryption of personal data. This is essential to protect the individuals' right to privacy and control over their personal information. Moreover, it helps to prevent the risk of profiling by judicial institutions.

Pursuant to this, work needs to be carried out on two fronts. The first is to establish a comprehensive and dependable database of judicial rulings. The second imperative is the assurance of adherence to constitutional principles and individual rights when implementing AI systems.

It is not feasible to merely substitute the natural judge with automatic predictive justice systems, regardless of any technological advancements. Citizens retain their fundamental right to access an independent and unbiased judge, established by law, in order to safeguard their rights.

However, the usefulness of AI systems cannot be denied in assisting judges in performing their duties. These systems include state-of-the-art search engines, software for drafting legal documents, automated systems to streamline internal work processes as well as software for easy perusal and filtering of information. They are also useful in handling simple, serial, repetitive, purely documentary cases, among others. AI systems could prove useful in alternative dispute resolution procedures when citizens freely choose them to expedite certain justice processes, particularly those related to administration and civil matters.

It would be unwise to neglect the potential benefits brought by information technology and new AI systems. When used in a carefully controlled manner, they could facilitate the enhancement of both quality and efficiency within our justice system. Moreover, they have the potential to lure greater amounts of industrial capital investment from abroad.

138. Cappelletti 1969, p. 569.

References

E.A. Afendras, N.S. Tzannes, J.G. Trépanier (1973), *Distance, Variation and Change in Phonology: Stochastic Aspects*, in "Folia linguistica", vol. 6, 1973, n. 1-2

E. Agazzi (1980) (ed.), *Modern Logic. A Survey*, Springer, 1980

C.E. Alchourrón, A.A. Martino (1990), *Logic without Truth*, in "Ratio Juris", vol. 3, 1990, n. 1

E. Amodio (2016), *Estetica della giustizia penale*, Giuffrè, 2016

C. Barbaro (2018), *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in "Questione giustizia", 2018, n. 4

G.A. Barnard (1955), *Statistical Calculation of Word Entropies for Four-Western Languages*, in "IRE Transactions on Information Theory", vol. 1, 1955, n. 1

F. Battaglia (2007), *Catene di Markov*, in Id., "Metodi di previsione statistica", Springer, 2007

J. Bernstein (1990), *Uomini e macchine intelligenti*, Adelphi, 1990

E. Betti (1948), *Le categorie civilistiche dell'interpretazione*, in "Rivista italiana per le scienze giuridiche", Giuffrè, 1948

R. Bin (2013), *A discrezione del giudice. Ordine e disordine: una prospettiva "quantistica"*, FrancoAngeli, 2013

M.A. Boden (2018), *Artificial Intelligence: A Very Short Introduction*, Oxford University Press, 2018

P. Bourdieu (2005), *The Practical Sense* (tr. it.), Armando, 2005

M. Brady (2013), *Emotional Insight: The Epistemic Role of Emotional Experience*, Oxford University Press, 2013

P. Calamandrei (1965), *Processo e democrazia*, in M. Cappelletti (a cura di), "Opere giuridiche", vol. 1, Morano Editore, 1965

P. Calamandrei (1954), *La crisi della giustizia*, in Aa.Vv., "La crisi del diritto", Cedam, 1954

M. Cappelletti (1969), *Processo e ideologie*, il Mulino, 1969

A. Carleo (2019) (a cura di), *Decisione Robotica*, il Mulino, 2019

A. Carleo (2018) (a cura di), *Il vincolo giudiziale del passato*, il Mulino, 2018

A. Carleo (2017) (a cura di), *Calcolabilità giuridica*, il Mulino, 2017

S.B. Carroll (2006), *Infinite forme bellissime. La nuova scienza dell'Evo-Devo*, Codice Edizioni, 2006

C. Casonato (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in "Diritto pubblico comparato ed europeo", 2019, n. 1s

S. Cassese (2022), *Il governo dei giudici*, Laterza, 2022

C. Castelli, D. Piana (2018), *Giustizia predittiva. La qualità della giustizia in due tempi*, in "Questione giustizia", 2018, n. 4

A. Celotto (2019), *I robot possono avere diritti?*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

A. D'Aloia (2019), *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

D. Dalfino (2019), *Stupidità (non solo) artificiale, predittività e processo*, in "Questione giustizia", 3 luglio 2019

S. Danziger, J. Levav, L. Avnaim-Pesso (2011), *Extraneous factors in judicial decision-making*, in "Pnas", vol. 108, 2011, n. 17

D. Davidson (1980), *Mental Events*, in Id., "Essays on Actions and Events", Clarendon press, 1980 (in Italian: *Eventi Mentali*, in "Azioni ed eventi", il Mulino, 1992)

A. de Tocqueville (1840/1968), *La democrazia in America*, II, transl.it., Utet, 1968

G.B. Debiasi, G.A. Valli (1968), *Sorgenti di messaggi per prove di intelligibilità della parola*, in "Atti e memorie dell'Accademia patavina di scienze, lettere ed arti", vol. 80, 1968

L. De Renzis (2019), *Primi passi nel mondo della giustizia «high tech»: la decisione in un corpo a corpo virtuale fra tecnologia e umanità*, in A. Carleo (2019) (a cura di), "Decisione Robotica", il Mulino, 2019

O. Dominioni (2005), *La prova scientifica penale. Strumenti tecnico-scientifici nuovi o controversi e altamente specializzati*, Giuffrè, 2005

D. Eagleman (2016), *The Brain: The Story of You*, Canongate Books Ltd, 2016

T. Eichinger (2018), *The Corpus Replication Task*, in "Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI)", IEEE Computer Society, 2018

P. Ekman (1999), *Introduzione*, in C. Darwin, "L'espressione delle emozioni nell'uomo e negli animali", Bollati Boringhieri, 1999

P. Ekman, H. Oster (1979), *Facial Expressions of Emotion*, in "Annual Review of Psychology", vol. 30, 1979

M. Fasan (2019), *Intelligenza artificiale e pluralismo: Uso delle tecniche di profilazione nello spazio pubblico democratico*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

L. Ferrajoli (2013), *Nove massime di deontologia giudiziaria*, in "Una Città", 2013, n. 208

M. Ferrarese (2017), *Decisional processing on parking behaviour in entropic settings*, in "Archives of Transport", vol. 41, 2017, n. 1

G. Fiandaca (2013), *Sul ruolo delle emozioni e dei sentimenti nella genesi e nella applicazione delle leggi penali*, in O. Di Giovine (a cura di), "Diritto penale e neuroetica", Cedam, 2013

K.A. Findley, M.S. Scott (2006), The multiple dimensions of tunnel vision in criminal cases, in "Wisconsin Law Review", 2006

A. Forza, G. Menegon, R. Rumiati (2017), *Il giudice emotivo. La decisione tra ragione ed emozione*, il Mulino, 2017

J. Frank (1930/2009), *Law and the Modern Mind*, Routledge, 2009

S. Fuselli (2013), *Le emozioni nell'esperienza giuridica: l'impatto delle neuroscienze*, in L. Palazzini, R. Zannotti (a cura di), "Il diritto nelle neuroscienze. Non 'siamo' i nostri cervelli", Giappichelli, 2013

E. Gabrielli, U. Ruffolo (2019), *Artificial intelligence and law*, in "Giurisprudenza italiana", 2019, n.

A. Garapon, J. Lassègue (2018), *Justice Digitale. Revolution graphique et rupture anthropologique*, Presses Universitaires de France - PUF, 2018

H. Gintis, D. Helbing (2013), Homo socialis*: an analytical core for socio-logical theory*, 2013

M.P. Golding (2001), *Legal reasoning*, Encore Edition, 2001

D. Goleman (1995), *Emotional Intelligence: Why it can matter more than IQ*, Bloomsbury, 1995

I. Goodfellow, Y. Bengio, A. Courville (2016), *Deep Learning*, The MIT Press, 2016

G. Gulotta (2014), *Psicologia dell'errore nell'investigazione e nel giudizio*, in L. De Cataldo Neuburger (a cura di), "'L'operazione decisoria'. Da emanazione divina alla prova scientifica. Passando per Rabelais", Cedam, 2014

G. Gulotta (2011), *Compendio di psicologia forense, criminale e investigativa*, Giuffrè, 2011

P. Hadot (2007), *Wittgenstein and the Limits of Language*, Bollati Boringhieri, 2007

P.R. Halmos (1974), *Naive Set Theory*, Springer, 1974

H.L.A. Hart (1961), *Il concetto di diritto*, Einaudi, 1961

G.E. Hughes, M.J. Cresswell (1996), *A New Introduction to Modal Logic*, Routledge, 1996

M. Iaselli (2024), *AI Act. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, 2024

F. Imposimato (2009), *L'errore giudiziario. Aspetti giuridici e casi pratici*, Giuffrè, 2009

N. Irti (2019), *Il tessitore di Goethe (per la decisione robotica)*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

N. Irti, E. Severino (2001), *Dialogo su diritto e tecnica*, Laterza, 2001

N. Irti, E. Severino (2000), *Le domande del giurista e le risposte del filosofo (un dialogo tra diritto e tecnica)*, in "Contratto e impresa", 2000, n. 2

S. Jasanoff (1995), *La scienza davanti ai giudici*, Giuffrè, 1995

D. Kahneman (2012), *Thinking, Fast and Slow*, Newyord Macmillan, 2012 (tr. it. *Pensieri Lenti e Veloci*, Mondadori)

L. Kalb (2005), *La "ricostruzione orale" del fatto tra "efficienza" ed "efficacia" del processo penale*, Giappichelli, 2005

J. Kaplan (2018), *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press 2018

A. Kilgarriff (1997), *I don't believe in word senses*, in "Computers and the Humanities", vol. 31, 1997, n. 2

A. Kozinski (1993), *What I Ate for Breakfast and Other Mysteries of Judicial Decision Making*, in "Loyola of Los Angeles Law Review", vol. 26, 1993, n. 4

L. Lanza (2011), *Emozioni e libero convincimento nella decisione del giudice penale*, in "Criminalia. Annuario di scienze penalistiche", 2011

J. Ledoux (1998), *The Emotional Brain: The Mysterious Underpinnings of Emotional Life*, Simon & Schuster, 1998

E. Livni (2017), *Nei tribunali del New Jersey è un algoritmo che decide chi esce su cauzione*, in "Internazionale.it", 3 marzo 2017

S. Lloyd (2006), *Il programma dell'universo*, Einaudi, 2006

M.G. Losano (1978), *L'informatica nell'Europa Orientale e l'opera di Viktor Knapp*, in V. Knapp, "L'applicabilità della cibernetica al diritto", Einaudi, 1978

M.G. Losano (1971), *Il primo anno del Centro di Giuscibernetica dell'Università di Torino*, in "Rivista internazionale di filosofia del diritto", 1971, n. 1

M.G. Losano (1969), *Giuscibernetica: macchine e modelli cibernetici nel diritto*, Einaudi, 1969

M.G. Losano (1967), *Cibernetica e diritto in Europa*, in "Il ponte", vol. 23, 1967, n. 12

M.G. Losano (1966-1967), *Giuscibernetica*, in R. Treves (a cura di), "Nuovi sviluppi della sociologia del diritto", Edizioni di comunità, 1966-1967

N. Luhmann (1990), *Sistemi sociali. Fondamenti di una teoria generale* (tr. it.), il Mulino, 1990

S.L. Lustig, K. Delucchi, L. Tennakoon et al. (2007), *Burnout and Stress Among United States Immigration Judges*, in "Bender's Immigration Bulletin", 2007, n. 22

R. Manfrino (1960), *L'entropia della lingua italiana ed il suo calcolo*, in "Alta frequenza", vol. xxix, 1960

C. Mangione, S. Bozzi (1993), *Storia della logica. Da Boole ai giorni nostri*, Garzanti, 1993

C. Manning, H. Schütze (1999), *Foundations of statistical natural language processing*, MIT press, 1999

V. Marzocco (2018), *Nella mente del giudice. Il contributo di Jerome Frank al realismo giuridico americano*, Giappichelli, 2018

C. Maslach, W.B. Schaufeli, M.P. Leiter (2001), *Job Burnout*, in "Annual Review of Psychology", vol. 52, 2001

T. Mazzarese (1996), *Forme di razionalità delle decisioni giudiziali*, Giappichelli, 1996

C. Minnaja, L.Paccagnella (1977), *Variazioni dell'entropia linguistica dell'italiano scritto e calcolo di un'entropia fonematica*, in "Rendiconti del Seminario Matematico della Università di Padova", vol. 57, 1977

C.J.A. Mittermaier (1846), *Della differenza fra delitti consumati e tentati, e dei gradi del conato*, in F.A. Mori (a cura di), "Scritti germanici", A. Nanni ed., 1846

M.A. Montemurro (2014), *Quantifying the information in the long-range order of words: Semantic structures and universal linguistic constraints*, in "Cortex", vol. 55, 2014

M.A. Montemurro, D.H. Zanette (2010), *Towards the quantification of the semantic information encoded in written language*, in "Advances in Complex Systems", vol. 13, 2010, n. 2

M.A. Montemurro (2009), *The statistics of meaning: Darwin, Gibbon and Moby Dick*, in "Significance", vol. 6, 2009, n. 4

M.A. Montemurro, D.H. Zanette (2005), *Dynamics of Text Generation with Realistic Zipf's Distribution*, in "Journal of Quantitative Linguistics", vol. 12, 2005, n. 1

J. Nieva-Fenoll (2019), *Intelligenza artificiale e processo*, Giappichelli, 2019

C. Nordio (2022), *Giustizia ultimo atto. Da Tangentopoli al crollo della magistratura*, Guerini e Associati, 2022

R. Orestano (1987), *Introduzione allo studio del diritto romano*, il Mulino, 1987

A.G. Orofino (2002), *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in "Il Foro Amministrativo C.d.S.", 2002, n. 9

P. Otranto (2018), *Decisione amministrativa e digitalizzazione della p.a.*, in "federalismi.it", 2018, n. 2

P.P. Paulesu (2008), *La presunzione di innocenza, tra realtà processuale e dinamiche extra processuali*, in A. Balsamo, R. Kostoris (a cura di), "Giurisprudenza europea e processo penale italiano", Giappichelli, 2008

G. Pisapia (1989), encyclopedic voice: *Errore giudiziario (riparazione dell')*. Diritto processuale penale, in "Enciclopedia Giuridica", vol. XIII, Ist. della Enciclopedia Italiana G. Treccani, 1989

R. Pound (1908), *Mechanical Jurisprudence*, in "Columbia Law Review", vol. 8, 1908, n. 8

H. Putnam (1987), *Mind, Language and Reality*, Adelphi, 1987

S. Quatrocolo (2019), *Equo processo penale e sfide della società algoritmica*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

R. Rordorf (2018), *Editoriale*, in "Questione giustizia", 2018, n. 3

A. Ross (1965), *Diritto e giustizia*, Einaudi, 1965

B. Russell (1914), *Our Knowledge of External World*, Allen and Unwin, 1914 (tr. it.: *La conoscenza del mondo esterno*, Longanesi, 1966)

G. Ryle (2009), *The Concept of Mind*, Routledge, 2009

S. Sabetta (2008), *Computazione ed entropia del sistema normativo*, in "complexlab.it", 2008

F. Saitta (2003), *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, in "Rivista di Diritto Amministrativo Elettronico", luglio 2003

G. Sartor (2005), *Legal Reasoning. A Cognitive Approach to the Law*, Springer, 2005

G. Sartor (2003), *Cognitive automata and the law*, in "The Law of Electronic Agents", Unipubskriftserier, 2003

F. Schauer (2000), *Le regole del gioco. Un'analisi filosofica delle decisioni prese secondo le regole nel diritto e nella vita quotidiana*, il Mulino, 2000

H. Schmid (1994), *Probabilistic Part-of-Speech Tagging Using Decision Trees*, in "Proceedings of International Conference on New Methods in Language Processing", 1994

J.R. Searle (1995), *The Construction of Social Reality*, Free Press, 1995

J.R. Searle (1984), *Intentionality and Its Place in Nature*, in "Dialectica", vol. 38, 1984, n. 2-3

E. Severino (2013), *La potenza dell'errare*, Rizzoli, 2013

S. Shalev-Shwartz, S. Ben-David (2014), *Understanding Machine Learning: From Theory to Algorithms*, Cambridge University Press, 2014

C.E. Shannon (1951), *Prediction and Entropy of Printed English*, in "The Bell System Technical Journal", vol. xxx, 1951

C.E. Shannon (1948), *A Mathematical Theory of Communication*, in "Bell System Technical Journal", vol. 27, July-October, 1948

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

L. Solum (2019), *Artificially Intelligent Law*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

F. Stella (2001), *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Giuffrè, 2001

E. Stradella (2019), *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in "MediaLaws", 2019, n. 1

P.F. Strawson (1961), *Introduzione alla logica teorica*, Einaudi, 1961

M. Tegmark (2018), *Vita 3.0 Esseri umani nell'era dell'intelligenza artificiale*, Raffaello Cortina Editore, 2018

M. Trifone (2009), *Il linguaggio burocratico*, in Id. (a cura di), "Lingua e identità. Una storia sociale dell'italiano", Carocci, 2009

P. Troisi (2011), *L'errore giudiziario tra garanzie costituzionali e sistema processuale*, Cedam, 2011

R.C. Van Caenegem (1991), *I signori del diritto* (tr. it), Giuffrè, 1991

Various Authors (2019), *Intelligenza Artificiale e diritto*, in "Giurisprudenza italiana", 2019, n. 7

Various Authors (1986), *Linguaggio e giustizia*, Nuove Ricerche, 1986

Various Authors(1975), *Italian speech synthesis from unrestricted text for an automatic answerback system*, in "Proceedings of the 8th International Congress on Acoustics", Chapman and Hall, 1975

Various Authors (1974), *Voice from computers: development prospects and reality of an application*, in "Proceedings of the 3rd Conference on Cybernetics and Biophysics", 1974

L. Viola (2018), *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in "federalismi.it", 2018, n. 21

F. Viola, G. Zaccaria (2003), *Le ragioni del diritto*, il Mulino, 2003

G.H. von Wright (1989), *Norma e azione. Un'analisi logica*, il Mulino, 1989

L. Wittgenstein (1967), *Tractatus logico-philosophicus*, Einaudi, 1967

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0203 • articolo sottoposto a peer review • pubblicato in anteprima il 29 apr. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Leonardo Marchesin

Oltre il consenso. I limiti dell'*Individual Control Model* e prospettive per un approccio collettivistico alla sorveglianza contemporanea

La sorveglianza contemporanea non ha portato soltanto vantaggi alle società post-moderne. Le attività di *dataveillance*, *data mining* e *profiling* rappresentano un pericolo reale nella maggior parte delle comunità umane odierne. Tale rischio riguarda non soltanto gli individui, vittime quotidiane di discriminazioni o visioni distorte della realtà, ma anche la collettività democratica in cui essi vivono, esposta alla progressiva erosione dei suoi principi fondamentali e delle pratiche dialogiche di cui si nutre. L'approccio tradizionale alla privacy e alla sua tutela (c.d. *Individual Control Model*) tenta, come dimostrato soprattutto dalla logica del consenso insufflata dal legislatore europeo nella disciplina del GDPR, di reagire a tale situazione di allarme riponendo tutte le proprie speranze nel rafforzamento del singolo e dei suoi diritti. Tuttavia, prassi quotidiane e studi scientifici hanno dimostrato l'inefficacia di un simile orientamento, il quale, da solo, rischia di peggiorare una condizione già emergenziale. Si rende, dunque, necessario un mutamento di paradigma, ovvero l'elaborazione di un sistema complessivo che, affiancandosi a quello già esistente, riesca a garantire una protezione effettiva delle persone e della loro privacy. Poiché, infatti, i pericoli generati dalla *dataveillance* riguardano non soltanto il soggetto ma anche la comunità intera, è necessario iniziare a pensare a delle risposte alla sorveglianza contemporanea che si avvalgano anche e soprattutto della forza collettiva del *demos* (c.d. *Societal Structure Model*).

Sorveglianza – Dataveglianza – Riservatezza – Individual Control Model – Societal Structure Model

Beyond the consent. The limits of the Individual Control Model and prospects for a collectivist approach to contemporary surveillance

Contemporary surveillance has not only brought benefits to post-modern societies. Dataveillance, data mining and profiling pose a real danger in most of today's human communities. This risk affects not only individuals, who are daily victims of discriminations or distorted views of reality, but also the democratic community in which they live, exposed to the progressive erosion of its fundamental principles and the dialogical practices on which it is nourished. The traditional approach to privacy and its protection (the so-called Individual Control Model) attempts, as demonstrated above all by the logic of consent insufflated by the European legislator in the GDPR regulation, to react to this situation of alarm by placing all its hopes in the empowerment of the individual and his rights. However, daily practices and scientific studies have demonstrated the ineffectiveness of this orientation, which, on its own, risks worsening an already emergency situation. What is needed, therefore, is a paradigm shift, i.e., the development of an overall system that, by complementing the existing one, is able to guarantee effective protection of individuals and their privacy. In fact, since the dangers generated by dataveillance concern not only the individual but also the entire community, it is necessary to start thinking of responses to contemporary surveillance that make use, also and above all, of the collective strength of the *demos* (so-called Societal Structure Model).

Surveillance – Dataveillance – Privacy – Individual Control Model – Societal Structure Model

L'Autore è tirocinante ex art. 73 l. 98/2013 presso il Tribunale Ordinario di Venezia

Sommario: 1. *Your browsing is being watched*. – 2. Il lato oscuro della sorveglianza. – 3. Lo stato dell'arte: l'*Individual Control Model*. – 4. Consenso senza senso. – 5. Agire, ma in quale direzione? – 6. Una prospettiva per il futuro: il *Societal Structure Model*.

1. *Your browsing is being watched*

La routinaria vita di tutti i giorni pare procedere in uno stato di quieta normalità, tanto per chi si affaccenda nelle più svariate attività lavorative o di studio, quanto per chi ancora gode degli ultimi attimi di festivo riposo. Eppure, tale idilliaco spaccato di quotidianità è destinato a subire una brusca e inquietante interruzione.

Dalla parete di un edificio pubblico, una telecamera si desta e, dispiegate le proprie ali metalliche, si distacca dal muro nel quale era stata precedentemente installata, planando rapidamente in prossimità di un individuo per osservarlo più da vicino. Dapprima uno solo, ma presto decine e decine di occhi elettronici compiono ammutinamento, abbandonano le rispettive posizioni all'interno dello scacchiere cittadino e si lanciano in una asfissiante persecuzione delle più svariate persone nelle quali hanno la ventura di imbattersi. A casa e in ufficio, nei parcheggi sotterranei e nelle fermate dei mezzi pubblici, addirittura nel lungomare e in un peschereccio al largo, nessuno può dirsi al riparo da questo stormo di telecamere che, come uccelli o pipistrelli, virano in picchiata verso qualsiasi soggetto capiti entro il loro campo visuale. L'obiettivo degli occhi elettronici è chiaro: spiare non tanto (o meglio, non solo) la persona in carne ed ossa, quanto piuttosto le attività che essa sta svolgendo attraverso l'iPhone che tiene costantemente nel palmo della propria mano.

A nulla sembrano valere la fuga, le urla di terrore, il getto a mare del proprio dispositivo o il tentativo velleitario di colpire le telecamere scagliandogli contro anche gli oggetti più improbabili. Gli occhi elettronici sono ovunque, e da essi non è dato trovare sicuro riparo.

Il quadro dalle tinte orwelliane dipinto da Apple nei pochi secondi dello spot che pubblicizza il motore di ricerca installato nei suoi dispositivi restituisce con poche ma incisive immagini uno stato dell'arte ben noto nell'ambito dei *surveillance studies*[1].

La dilagante presenza di CCTV e sistemi di videosorveglianza pubblici e privati all'interno dei tessuti urbani rappresenta una realtà radicata e persistente oramai da diversi decenni, tanto che già agli inizi del secolo Hille Koskela aveva modo di sostenere senza tema di smentita che "surveillance cameras are commonly used to protect high-class private premises – 'gated communities' – but also semi-public places such as shopping malls, underground and mainline train-stations, police stations and even churches" e "to monitor city streets"[2].

1. V. lo spot pubblicitario integrale.
2. Koskela 2000, p. 245. Negli stessi anni, in Italia, Stefano Rodotà parimenti affermava che "il semplice camminare per strada diventa un atto implacabilmente registrato da una telecamera, le informazioni vengono conservate ed ogni nostro passaggio in una piazza o in una strada, in una stazione, in un grande magazzino può essere ritrovato": Rodotà 2004, p. 173. E la diffusione dei sistemi di videosorveglianza che veniva rilevata a inizio secolo pare non accennare a diminuire o decelerare. In Italia, il *Rapporto Nazionale sull'attività della Polizia Locale* del 2023 ha infatti attestato che nel 2022, presso i 145 comandi analizzati, risultavano installate complessivamente 29.137 telecamere di videosorveglianza, in media 202 per ogni città,

Analogamente, non costituisce una recente novità la diffusione presso larga parte della popolazione mondiale di dispositivi elettronici in grado di perpetrare forme di monitoraggio destinate ad andare ben oltre la sola captazione di parole e condotte resa possibile dalla tradizionale videosorveglianza. Come noto, infatti, pressoché la totalità degli apparecchi tecnologici e dei software informatici quotidianamente utilizzati dalla maggior parte delle persone risulta essere capace di raccogliere, immagazzinare, assemblare ed elaborare dati e metadati emessi dagli utenti medesimi, ora volontariamente ora inconsapevolmente[3]. Non è, dunque, un caso che già sul finire del secolo scorso Roger Clarke avesse rilevato la presenza, accanto alla "classica" *surveillance*, di una *dataveillance*[4].

Tuttavia, come dimostrato dal summenzionato *spot* pubblicitario di Apple, il consolidamento nel tempo e nello spazio delle anzidette dinamiche di controllo e delle tecnologie che le rendono possibili non ha implicato una diminuzione dei timori connessi agli effetti di una sorveglianza che appare sempre più fluida, subdola e pervasiva.

Negli ultimi decenni, infatti, numerosi sono i giuristi, gli informatici, i sociologi e gli economisti che, nei rispettivi ambiti di studio, hanno levato incessantemente la loro voce specialistica per denunciare i rischi individuali e collettivi connessi alla vigilanza contemporanea, nonché per provare ad approntare soluzioni teoriche e pratiche volte ad arginarne le conseguenze maggiormente dirompenti e pregiudizievoli. E non è, dunque, un caso se oramai da tempo anche i legislatori di numerose nazioni e organizzazioni internazionali hanno deciso di intervenire normativamente per (provare a) regolare un contesto, quello della sorveglianza, tanto dannoso in potenza quanto diffuso nella pratica[5].

In questo articolo si procederà innanzitutto alla riepilogazione critica di quelli che, nell'ambito dei *surveillance studies*, sono notoriamente ritenuti gli effetti maggiormente pericolosi delle attuali forme di monitoraggio. L'attenzione verrà posta in particolar modo su quelle modalità di controllo che, ben più invasive rispetto alla mera videosorveglianza, hanno riguardo alla dimensione digitale della persona anziché al suo corpo fisico. In tale contesto, si avrà modo di evidenziare come simili conseguenze attentino non solo alle libertà e ai diritti del singolo individuo ma anche, e conseguentemente, ai valori e ai principi che fondano le società oggigiorno rette da una logica democratica.

Successivamente, e prendendo a modello anzitutto la regolamentazione racchiusa nel GDPR (*General Data Protection Regulation*, o Regolamento 2016/679), si darà spazio a una sintesi dei principali rimedi accolti e applicati a livello dottrinale prima e legislativo poi, evidenziando come questi ultimi si muovano entro un orizzonte perlopiù individualistico e scarsamente incline a considerare soluzioni di natura più marcatamente collettivistica. Sulla base di ciò, si avrà modo di riscontrare i patenti limiti che affliggono tale approccio fondato sull'esaltazione del potere e del controllo del singolo soggetto, i quali risulteranno manifesti una volta evidenziati i vizi logici e pratici che inficiano il concetto cardine in cui tale approccio si incarna, ovverosia quello del consenso.

Per concludere, si cercherà di mostrare come, al fine di provare ad arginare le conseguenze più

il che segna un netto aumento rispetto all'anno precedente, quando la media registrata è stata di 192 telecamere per ogni città.

3. L'esempio più celebre è dato dalla localizzazione operata dagli smartphone: "a meno di disattivarla esplicitamente all'interno del menù impostazione del vostro dispositivo […] la localizzazione non cessa di lasciare traccia di ogni vostro spostamento nel mondo […]. Algoritmi applicati alla velocità a cui vi muovete sono utilizzati per dedurre se siete a piedi o in macchina, o persino in quale tipo di veicolo vi trovate […]": Greenfield 2017, pp. 27-28.
4. Cfr. Clarke 1998, p. 499.
5. Tra le più celebri normative internazionali che si sono occupate della sorveglianza dei dati si ricordano le Linee Guida OCSE del 1980, la Convenzione 108 del Consiglio d'Europa (o Convenzione di Strasburgo) del 1981, il General Data Protection Regulation (GDPR), successore della Direttiva 95/46/CE (c.d. Direttiva Madre), e l'Asia-Pacific Economic Cooperation (APEC) del 2004. Di tutela della privacy, più in generale, si occupano anche la Dichiarazione universale dei diritti umani del 1948 (art. 12), la CEDU del 1950 (art. 8), il Patto internazionale sui diritti civili e politici del 1966 (art. 17) e la Carta di Nizza del 2000 (artt. 7, 8 e 52).

preoccupanti di una sorveglianza alla quale la logica dell'assenso risulta non essere stata in grado di porre freni tangibili e realmente efficaci, si renda necessario un mutamento di paradigma, quantomeno parziale. Se, infatti, non appare opportuno abbandonare *in toto* il modello consensuale attualmente prevalente sul piano normativo, è altrettanto necessario ammettere che continuare a fare affidamento esclusivamente sul medesimo rischia di dimostrarsi una scelta poco azzeccata alla luce dei risultati finora raggiunti. Appare, pertanto, opportuno iniziare a volgere lo sguardo anche verso misure di natura maggiormente collettivistica per far fronte a delle dinamiche di controllo che, in fin dei conti, non attentano soltanto alla persona ma anche alla società in cui essa vive.

2. Il lato oscuro della sorveglianza

Benché essa presenti taluni profili di favore per la società e di vantaggio per l'individuo[6], la sorveglianza, sia essa generalmente intesa ovvero considerata con specifico riferimento all'odierna epoca post-moderna, appare in grado di produrre effetti nocivi tali, per portata e propagazione, da dover essere – come sono stati e continuano ad essere – resi oggetto di attenta analisi.

L'ambiguità insita nel concetto stesso di monitoraggio[7], già evidente nelle consolidate pratiche di videosorveglianza[8], non pare affievolirsi o venire meno neppure allorquando la sorveglianza abbia ad oggetto non tanto le condotte materiali dell'individuo quanto piuttosto i dati virtuali che lo riguardano[9]. Anzi, le innovative modalità di controllo del corpo elettronico e dell'identità digitale della persona paiono, se possibile, accentuare i lati negativi della sorveglianza, benché i profili positivi della stessa continuino ad essere più appariscenti[10].

Come noto, la quotidianità della maggior parte dei soggetti che vivono nelle società contemporanee si dipana sempre più di frequente anche attraverso una dimensione virtuale[11]. Numerose sono le attività giornaliere che odiernamente si possono (o, addirittura, si devono) svolgere non più materialmente, bensì con l'ausilio di Internet e di dispositivi elettronici ad esso connessi[12]. Ed è altrettanto riconosciuto che nel momento in cui un individuo si trova ad agire all'interno della Rete

6. Ne sono un esempio paradigmatico i benefici apportati in ambito medico-sanitario dall'utilizzo dei dati: cfr. Orefice 2018, pp. 152-154.
7. L'ambiguità della sorveglianza è tema più volte sottolineato da David Lyon: cfr., tra gli altri, Lyon 2020, p. 91 ss. La natura ambivalente del monitoraggio pare addirittura accentuarsi se considerato in relazione al carattere altrettanto sfumato delle tecnologie che oggigiorno lo rendono possibile. Sull'ambiguità delle odierne tecnologie cfr. Stiegler 2023.
8. Da un lato, infatti, l'installazione di telecamere all'interno dei tessuti urbani viene giustificata, non senza sollevare perplessità, quale misura di tutela della sicurezza personale e cittadina (cfr. Svendsen 2017 e Lyon 2020, *passim*). Dall'altro lato, tuttavia, non è più un mistero che, qualora scorretto, sfuggente e orientato da pregiudizi, l'uso di occhi elettronici possa portare all'insorgenza di trattamenti discriminatori a danno di singoli soggetti o interi gruppi sociali, nonché alla disincentivazione finanche di pratiche tutt'altro che illecite e, anzi, funzionali all'esercizio di libertà democratiche (cfr. Greenfield 2017, p. 248, e Pin 2022, p. 7).
9. Cfr. De Kerkhove 2016, p. 36, e Orefice 2018, pp. 106-107.
10. In generale, David Lyon ritiene, riprendendo un linguaggio in uso già da tempo presso alcuni hacker, che oggi si possa parlare di *neofilia*: tale è la propensione delle persone a essere entusiaste delle novità apportare dalle nuove tecnologie, la quale le induce a dimenticare o sottovalutare i rischi che esse portano con sé, sorveglianza inclusa: cfr. Lyon 2020, p. 100 ss.
11. Celebri sono i due neologismi ideati da Luciano Floridi per indicare l'attuale dispiegarsi della vita umana tra dimensione analogica e dimensione digitale, ovverosia *inforg* (*informational organism*) e *onlife* (crasi di *online* e *life*): cfr., tra gli altri, Floridi 2020. Le due dimensioni sembrano destinate a fondersi con un grado di compenetrazione ancora maggiore a seguito dell'avvento del c.d. Metaverso, ovverosia la "possibilità di elevare il livello di interazione tra il mondo 'reale' e quello 'virtuale' fino al punto (ideale) in cui le esperienze vissute in essi siano totalmente coerenti e interscambiabili": Sarra 2024, p. 4.
12. Cfr. Delmastro–Nicita 2019, pp. 8-9, e Marchesin 2024-a, p. 31.

esso, volontariamente o meno, cede un gran numero di dati e rilascia un'ingente quantità di metadati (c.d. *big data*), prontamente raccolti, incasellati, assemblati e utilizzati non solo da istituzioni pubbliche ma anche da imprese private[13].

La realtà che è andata consolidandosi in anni recenti difficilmente potrebbe considerarsi del tutto negativa, in quanto foriera anche di possibilità e comodità di indubbio vantaggio[14]. Tuttavia, occorre ricordare che simili facilitazioni della vita individuale e collettiva implicano una ingente raccolta di informazioni da parte di attori pubblici e privati, i quali, pertanto, si avvalgono a tal fine di algoritmi e software in grado di controllare tutte le attività dell'utente e di tradurle in preziose strisce alfanumeriche dalle quali estrarre conoscenza (*data mining*, o *data analysis*)[15].

Come evidenziava già nella decade precedente Eli Pariser, l'attività di reperimento e conservazione di dati e metadati tramite algoritmi risulta essere funzionale al *profiling* della persona, ovverosia alla schedatura delle sue preferenze, idee ed opinioni e alla sua conseguente classificazione entro categorie predefinite (*data segments*)[16]. Ed è proprio una simile dinamica a suscitare, tra i *surveillance scholars*, i maggiori allarmi.

Dal punto di vista individuale, infatti, la targetizzazione implica una vera e propria reificazione del soggetto. La riduzione della multiforme personalità umana a un neutro coagulo di stringe alfanumeriche rappresenta un chiaro svilimento della dignità dell'individuo, il quale vede appiattite le proprie idee ed emozioni entro gli angusti spazi di un database elettronico atto alla sua successiva manipolazione[17].

E forse tale prassi potrebbe ancora considerarsi tollerabile qualora fosse funzionale alla mera facoltà di personalizzare le *app* e la grafica dei dispositivi. Tuttavia, il *profiling* non risulta essere fine a se stesso. Esso, infatti, rappresenta il principio sulla base del quale vengono prese decisioni destinate a incidere più o meno pesantemente sulla vita della persona (*data-driven society*)[18]. Non si tratta soltanto della possibilità di inoltrare messaggi pubblicitari personalizzati o di effettuare delle perfette discriminazioni di offerte e prezzi tra gli utenti (*behavioral retargeting*)[19]. In base al credito sociale che emerge dai dati raccolti, le decisioni assunte dagli algoritmi possono incidere sulla vita lavorativa e pubblica di un soggetto[20]. Sicché è evidente non solo la progressiva perdita di controllo sulle proprie vite da parte di utenti spesso inconsapevoli di tali

13. Sulla quantità di dati rilasciati da un utente medio ogni giorno cfr. Greenfield 2017, p. 29; Delmastro–Nicita 2019, pp. 10-11; Perri 2020, pp. xi-xii; Maestri 2021, p. 56; Pin 2021, p. 51; Paolucci 2021, p. 205; Sarra 2022-a, pp. 21-22; Pietropaoli 2024, p. 4; Marchesin 2024-a, pp. 31-32.
14. A livello collettivo, ad esempio, vale la pena notare che taluni reati difficilmente potrebbero essere perseguiti e, conseguentemente, sanzionati come per legge in assenza della possibilità, per le forze dell'ordine e per i pubblici ministeri, di acquisire file di log e di traffico telefonico incamerati dai dispositivi tecnologici impiegati dai rei. Sul piano individuale, analogamente, le amenità garantite dalle odierne tecnologie implicanti un certo grado di vigilanza risultano essere sin troppo evidenti.
15. Sulla definizione di *data mining* cfr. Maestri 2021, p. 60, e Sarra 2022-a, p. 84.
16. Cfr. Pariser 2012. Sulla profilazione e sul suo funzionamento cfr. anche Greenfield 2017, pp. 214-215, e Delmastro–Nicita 2019, p. 27.
17. Sugli effetti reificanti della sorveglianza contemporanea e sulla possibile correlazione tra essi e le conseguenze disumanizzanti e spersonalizzanti discendenti dal monitoraggio panottico di epoca moderna cfr. Marchesin 2024-b. Sulla reificazione dell'utente provocata dalla riduzione dell'essere umano in dati e dalla sorveglianza che li riguarda cfr. anche Orefice 2018, p. 79; Becker 2019, p. 311; Maestri 2021, p. 63; Han 2021, pp. 20-21; Paolucci 2021, p. 208; Han 2023, p. 13; Sarra 2024, p. 18; Pietropaoli 2024, p. 4.
18. Cfr. Sarra 2022-a, p. 85, e Sarra 2022-b, *passim*.
19. Cfr. Orefice 2018, pp. 105-106; Delmastro–Nicita 2019, pp. 11 e 81-83; Bazzoni 2019, p. 639; Pin 2021, p. 52; Di Corinto 2022, pp. 32-33; Ferraris–Saracco 2023, p. 46; Han 2023, pp. 27-28; Pietropaoli 2024, p. 4; Doctorow 2024, p. 20.
20. Cfr. Delmastro–Nicita 2019, p. 123, e Pin 2021, p. 56.

dinamiche[21], ma anche il pericolo di perpetrazione di pratiche discriminatorie e sperequative[22], posta la asserita non neutralità degli algoritmi utilizzati[23].

Da una prospettiva aperta all'intero consorzio umano, i rischi anzidetti non paiono affievolirsi.

La profilazione, infatti, permette di avvalersi delle preferenze personali emergenti dall'analisi dei dati per selezionare non solo le occasioni di lavoro e di acquisto, ma anche le notizie che ciascun individuo avrà modo di visualizzare, nonché l'ordine in cui esse appariranno ai suoi occhi (*self-sorting*). In un mondo dove il web e i social network costituiscono sempre più di frequente la principale fonte di informazione per un gran numero di persone[24], queste ultime sono destinate a venire a contatto pressoché esclusivamente con notizie che, secondo le previsioni di un algoritmo opaco, più si confanno alle loro idee e preferenze, ovverosia con informazioni che tendono a confermare – o, quantomeno, a non mettere in discussione – le loro opinioni originarie, giuste o errate che siano[25].

È innegabile che tale dinamica possa, entro certi termini, essere utile per mettere in comunicazione tra loro individui che condividono i medesimi interessi ma che vivono in luoghi tra loro assai distanti; tuttavia, essa cela pericoli estremamente elevanti per la collettività.

Divenute destinatarie pressoché in via esclusiva di informazioni sartorialmente ritagliate sulla base dei dati e metadati rilasciati in Rete, le persone corrono il rischio di entrare in possesso di una visione della realtà soltanto parziale o comunque ideologicamente orientata in base alle loro preferenze aprioristiche[26]. Il nocumento determinato da una simile situazione non riguarda soltanto i singoli soggetti, che sono esposti al pericolo di non poter accedere alla verità dei fatti e di essere privati del diritto a un'informazione imparziale e completa. A essere danneggiata è l'intera società, la quale dovrà sopportare gli effetti pregiudizievoli prodotti dalle decisioni prese dai suoi membri sulla base di notizie deficitarie, parziali e incomplete, se non addirittura del tutto false[27].

Non solo. Come sostiene Cass R. Sunstein, la reclusione degli individui entro impercettibili *filter bubbles* rischia di produrre effetti di "polarizzazione" e "frammentazione"[28] delle varie frange della popolazione. Se attraverso i più usati mezzi di informazione le persone rinverranno pressoché esclusivamente notizie confermative dei loro pensieri e pregiudizi, esse si trincereranno e radicalizzeranno attorno alle loro posizioni, divenendo sempre meno propense all'accoglimento o anche solamente all'ascolto di idee e opinioni diverse provenienti da gruppi sociali differenti[29] (c.d. autismo informativo[30]).

In questi termini – e ben al contrario rispetto a quanto si prospettava all'epoca dell'avvento di Internet[31] –, è evidente il pericolo corso dagli attuali regimi democratici, chiamati non solo a fronteggiare la disinformazione dei singoli soggetti ma anche a far fronte alla progressiva perdita di efficacia della pratica dialogica, da sempre collante del tessuto sociale.

21. Cfr. Solove 2021, p. 39, e Pietropaoli 2024, p. 5.
22. Cfr. Pin 2021, p. 57, e Pietropaoli 2024, p. 2.
23. Cfr. Greenfield 2017, pp. 239-240; Perri 2020, p. 132; Sarra 2022-a, p. 93; Kienke 2023, p. 49; Coniglione 2023, p. 3.
24. Cfr. Delmastro–Nicita 2019, pp. 91-93, e Han 2022, p. 32.
25. Cfr. Sunstein 2017, pp. 11-14; Delmastro–Nicita 2019, pp. 94-102; Bazzoni 2019, pp. 639-640; Sarra 2022-a, p. 94; Han 2023, p. 28.
26. Cfr. Pin 2021, pp. 52-53.
27. Sulla diffusione delle fake news e sulle sue conseguenze cfr. Moro–Fioravanzi 2022.
28. Sunstein 2017, p. 15.
29. Cfr. Sunstein 2017, pp. 21-22 e 37; Delmastro–Nicita 2019, pp. 101, 111; Bazzoni 2019, p. 641; Han 2023, pp. 39-40; Kienke 2023, pp. 42-43; Coniglione 2023, p. 10; Pietropaoli 2024, p. 5; Solove–Hartzog 2024, p. 1029. Tale pericolo si innesta, peraltro, nel contesto generale attuale, il quale, contraddistinto dalla rapidità delle informazioni, sovente priva del tempo necessario per instaurare dibattiti seri e approfonditi: cfr. Han 2023, p. 25.
30. Cfr. Kienke 2023, p. 46.
31. Cfr. Scorza 2022.

3. Lo stato dell'arte: l'*Individual Control Model*

Pur a fronte di uno scenario inquietante e apparentemente privo di speranza per la riservatezza degli individui, il summenzionato *spot* pubblicitario di Apple termina con un lieto fine. Cliccando sull'icona di Safari, infatti, le persone perseguitate dalle telecamere volanti riescono ad annientarle, sfuggendo così al loro penetrante e infaticabile sguardo. Il messaggio conclusivo è chiaro: *Safari. A browser that's actually private*.

È evidente il tentativo dello *spot* pubblicitario del motore di ricerca impiegato da Apple di esporre al pubblico la volontà della multinazionale statunitense di attuare forme di *privacy by design e privacy by default*. Tuttavia, esso dipinge un suggestivo quadro ben indicativo di un certo approccio alla tutela della riservatezza: soggetti consapevoli di essere costantemente sorvegliati da dispositivi implacabili – rappresentati dagli occhi elettronici muniti di ali –, preoccupati se non addirittura terrorizzati da tale situazione complessiva, decidono scientemente di adottare comportamenti volti alla protezione della loro privacy – esemplificati in estrema sintesi dal gesto di cliccare sull'icona di Safari.

Nell'ambito dei *surveillance studies* è frequente imbattersi in proposte che mirano a osteggiare le più invasive forme di monitoraggio e i loro effetti maggiormente intollerabili attraverso pratiche che fanno affidamento sul singolo, ovvero su circoscritti gruppi di soggetti mossi da iniziative individualistiche.

In riferimento alla videosorveglianza, ad esempio, Cossutta e Mainardi ritengono lodevole ed efficace l'attività politico-artistica di collettivi quali i *Surveillance Camera Players*, un gruppo i cui membri "organizzano performance-protesta di fronte alle camere di sorveglianza situate in luoghi pubblici e […] usano la loro visibilità, le loro apparizioni pubbliche, le loro interviste e il loro sito per sfatare il luogo comune che 'solo chi è colpevole di qualcosa si oppone alla sorveglianza'"[32]. Relativamente al contesto digitale, invece, è nota la proposta di Brunton e Nissenbaum, divenuta celebre come "offuscamento": incentivati a cliccare su qualsivoglia *banner* sia presente nelle pagine web visitate (*AdNauseam*) o a rilasciare un'ingente quantità di like a prescindere dal contenuto dei post pubblicati nei social network (*like-farming*), gli individui vengono invitati, attraverso queste e altre condotte analoghe, all'"aggiunta deliberata di informazioni ambigue, confuse e ingannevoli per interferire con la sorveglianza e la raccolta di dati personali"[33].

Analogamente, e sempre avuto riguardo alla sorveglianza dei dati, a livello normativo si riscontra oramai da decenni una generale adesione dei legislatori a quello che, in letteratura, viene definito *Individual Control Model*, ovverosia un'impostazione generale che – per usare le parole del suo più noto teorizzatore, Alan F. Westin – considera la privacy come "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"[34]. In altri termini, a fronte di un generale depotenziamento (*disempowerment*) dell'individuo causato dalle nuove tecnologie e dalla sorveglianza che esse permettono, lo scopo perseguito da numerosi legislatori è quello di adottare misure normative volte a favorire un rafforzamento (*empowerment*) del singolo soggetto, garantendogli diritti specifici e, in generale, un maggiore controllo sui suoi dati[35].

Tale approccio alla riservatezza e alla sua tutela, invalso anche negli Stati Uniti a partire dagli anni Settanta del secolo scorso[36], trova oggi la sua

32. Cossutta–Mainardi 2018, p. 173.

33. Brunton–Nissenbaum 2016, p. 10.

34. Westin 1967, p. 7. Come rileva Julie Zahle, la visione secondo cui il miglior strumento di tutela della privacy è rappresentato dal consenso informato ha avuto un notevole successo, tanto da continuare ad essere perorata ancora in tempi recenti: cfr. Zahle 2017, p. 1.

35. Cfr. Hartzog 2018-a, pp. 423-425; Richards–Hartzog 2019, p. 1462; Becker 2019, pp. 308-309; Solove–Hartzog 2024, pp. 1023-1025; Elvy 2024, p. 644.

36. Già nel 1973 lo U.S. Department of Health, Education, and Welfare decise di trasfondere la logica dell'*individual control model* in un report poi rivelatosi assai influente, secondo il quale gli individui avrebbero dovuto avere "a right to participate in deciding what the content of the record will be, and what disclosure and use

massima espressione nella normativa in materia di privacy più celebre a livello internazionale, ovverosia nel GDPR entrato in vigore il 25 maggio 2018 nel contesto eurounitario[37].

Coerentemente con il dichiarato intento di assicurare un maggior controllo all'individuo sui dati che lo riguardano (Considerando 7 GDPR)[38], il Regolamento 2016/679 riconosce un'ingente numero di diritti al singolo soggetto, garantendogli la possibilità non solo di cederli, ma anche di accedervi (art. 15, parr. 1 e 3, GDPR), rettificarli/integrarli (art. 16 GDPR), richiederne la cancellazione (art. 17 GDPR) ovvero il trasferimento (art. 20 GDPR).

Non solo. La massima espressione dell'adesione del *General Data Protection Regulation* a un'ottica ispirata all'*Individual Control Model* è data dal notevole affidamento che esso compie nei confronti del consenso individuale quale "potente strumento di controllo e partecipazione del singolo nella gestione delle proprie informazioni"[39].

Come noto, l'assenso individualmente prestato non rappresenta la sola base giuridica in grado di legittimare il trattamento dei dati da parte di titolari e responsabili dello stesso[40]. Sono previste, infatti, altre cinque condizioni di legittimità del trattamento, le quali prescindono totalmente dal consenso individuale e devono ritenersi analoghe ad esso per valenza. Sicché, soprattutto con l'avvento del GDPR, è possibile affermare che oggi l'assenza dell'assenso individualmente prestato non preclude necessariamente la liceità del trattamento dei dati, qualora ricorra nel caso concreto una diversa base giuridica[41]. Anzi, è possibile affermare, con Andrea Maria Garofalo, che tale condizione di liceità del trattamento deve ritenersi astrattamente residuale, in quanto destinata a trovare attuazione laddove non sia possibile dare applicazione alle altre previste dal Regolamento 2016/679[42].

Tuttavia, proprio in virtù della sua natura residuale, il consenso individuale costituisce in concreto la base giuridica più di frequente impiegata nella prassi quotidiana; sicché non deve meravigliare che essa emerga complessivamente dal *General Data Protection Regulation* quale prima e principale condizione di legittimità delle pratiche volte alla raccolta, all'immagazzinamento e all'utilizzo di dati relativi alla persona[43]. Da un lato, vale sottolineare che il consenso dell'interessato è menzionato dall'art. 6, par. 1, GDPR quale prima base giuridica

will be made of the identifiable information in it": cfr. U.S. Department of Health, Education & Welfare 1973, p. 41.

37. Come sottolinea Fausto Caggia, la decisione di sostituire la previgente Direttiva Madre 95/46/CE con un Regolamento si spiega anche alla luce della volontà del legislatore europeo di unificare le normative statuali in materia di privacy, nonché le prassi commerciali e i codici di condotta concernenti attività svolte con l'ausilio del web: cfr. Caggia 2019, pp. 431-432.
38. Cfr. Maestri 2021, p. 66, e Sarra 2022-b, p. 45.
39. Meneghetti 2021, p. 276. Cfr. anche Solove–Hartzog 2024, p. 1030, e Marchesin 2024-a, pp. 33-34. In tale frangente, il GDPR si pone in continuità rispetto alla previgente Direttiva 95/46/CE: cfr. Meneghetti 2021, pp. 268-269.
40. L'art. 6, par. 1, GDPR prevede altre cinque basi di legittimità del trattamento dei dati: l'esecuzione di contratti e misure precontrattuali di cui l'interessato è parte; l'adempimento di un obbligo legale da parte del titolare del trattamento; la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica; l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri da parte del titolare del trattamento; il perseguimento di interessi legittimi dello stesso. Cfr. Bravo 2017, p. 138 ss.
41. Come nota Dianora Poletti, "la possibilità di (facile) revoca [del consenso individuale], espressamente indicata dall'art. 7, par. 3, Regolamento […], impedisce la prosecuzione del trattamento che su di esso si fondava, a meno che il titolare non faccia valere una condizione di liceità alternativa": Poletti 2019, p. 2785.
42. Cfr. Garofalo 2021, p. 121, nota 8.
43. Cfr. Seminara 2021, pp. 860-861; Meneghetti 2021, p. 267; Coniglione 2023, p. 6; Solove 2024, p. 596; Sarra 2024, p. 20. Sulla posizione di chi ritiene che il legislatore europeo, pienamente consapevole del funzionamento delle odierne economie di rete, abbia inteso, attraverso il GDPR, sminuire il ruolo centrale rivestito dal consenso individuale in materia di privacy cfr. Caggiano 2017, p. 15, e Caggia 2019, pp. 405-410.

funzionale alla legittimità del trattamento dei dati, e che esso soltanto tra le basi giuridiche riceve una definizione specifica *ex* art. 4 GDPR[44]. Dall'altro lato, come osserva acutamente Alessandro Purpura, "la manifestazione di consenso ad opera dell'interessato basterebbe ad escludere una valutazione di necessità del trattamento prevista invece in tutti gli altri casi"[45]; con ciò dimostrando la volontà del legislatore europeo di riconoscere una forza quasi insindacabile all'assenso dell'interessato. Inoltre, come ricorda Dianora Poletti, non solo "il consenso sembra rafforzarsi nella sua modalità di manifestazione, divenendo 'esplicito' e 'inequivocabile'", ma esso "riveste un ruolo decisivo nel caso (rilevante soprattutto per le applicazioni di intelligenza artificiale) del trattamento automatizzato dei dati personali (art. 22)"[46].

Benché si sia, dunque, cercato di prendere progressivamente le distanze dalla logica del trattamento dei dati basata in via esclusiva sulla nozione di consenso individuale, *in primis* prevedendo nuove e più stringenti basi giuridiche, l'assenso dell'interessato continua a ricevere notevole attenzione da parte del legislatore europeo – certamente più di quanta ne ricevano le altre condizioni di legittimità[47]. Sicché, se da un lato ciò dipende dalla diffusione spazio-temporale della prassi consensuale, dall'altro lato una simile scelta legislativa non può che finire per conservare – se non addirittura implementare – tale stato dell'arte.

La fiducia ancora riposta dal GDPR nel consenso individuale ben si evince, poi, dall'attenzione dedicata dal legislatore europeo alla sua disciplina, tanto da pervenire al punto di dedicarvi una definizione assai puntuale e articolata.

Per consenso, infatti, il Regolamento 2016/679 intende "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (art. 4, n. 11, GDPR). Benché non sia chiamato a integrare una forma specificamente predeterminata[48] – fatta eccezione, soprattutto, per le ipotesi concernenti dati sensibili, nelle quali se ne richiede la natura esplicita (art. 9, par. 2, lett. a, GDPR) –, il consenso deve integrare quattro requisiti per potersi dire valido e legittimante: a) la libertà, sinonimo di consapevolezza del consenso da parte dell'utente e di assenza di coartazione al momento della sua prestazione (Considerando 42 GDPR)[49]; b) la specificità, collegata al principio di minimizzazione dei dati, in virtù del quale il consenso deve essere "limitato, pertinente ed adeguato a quanto necessario rispetto alle finalità per le quali [i dati] sono trattati" (art. 5 GDPR)[50]; c) l'informazione, che

44. Alessandro Purpura, inoltre, evidenzia come l'attenzione riservata dal legislatore europeo alla disciplina della validità del consenso individuale sia sintomo della sua perdurante centralità nel quadro del GDPR: cfr. Purpura 2022, p. 904.
45. Purpura 2022, p. 901. Ciò deve considerarsi vero anche allorquando si tratti di derogare ai divieti al trattamento di dati personali e genetici previsto dall'art. 9, par 1, GDPR, purché il consenso individuale sia esplicito. Sulla centralità del consenso emergente dalla disciplina dell'art. 9 GDPR cfr. Tuccari 2024, p. 517.
46. Poletti 2019, p. 2785. Sulla rilevanza del consenso individuale nel trattamento automatizzato di dati personali cfr. anche Troisi 2019, p. 45.
47. Se da un lato il GDPR, ammettendo anche altre basi giuridiche, dà prova della consapevolezza del legislatore europeo che non sempre gli individui sono effettivamente capaci di tutelare i propri dati, dall'altro lato continua a riconoscere la rilevanza del consenso individuale, permettendo ai singoli soggetti di disporre delle informazioni che li riguardano: cfr. Garofalo 2021, p. 119.
48. Così risulta dalla lettura del considerando 32 e dell'art. 7 GDPR. Tale profilo rappresenta oggetto di consolidata dottrina in questo senso: cfr. Caggiano 2017, p. 10; Caggia 2019, pp. 414-416; Seminara 2021, p. 864. In questi termini, il GDPR ha innovato quanto precedentemente previsto dal Codice privacy italiano, che, prima dell'entrata in vigore del Regolamento europeo, faceva ambiguamente riferimento alla forma scritta del consenso all'art. 23, co. 3, Codice privacy (oggi abrogato).
49. Cfr. Seminara 2021, p. 865, e Meneghetti 2021, p. 274.
50. Connesso alla specificità del trattamento dei dati è il principio che ne richiede la granularità: cfr. Seminara 2021, p. 863.

deve essere fornita all'interessato dal titolare del trattamento in maniera accessibile, chiara e comprensibile non solo in merito alle finalità e al contenuto del processamento dei dati raccolti (artt. 13 e 14 GDPR) ma anche relativamente ai diritti esercitabili dall'interessato stesso (artt. 15-22 GDPR)[51]; d) l'inequivocabilità, connessa alla necessità di espressione del consenso attraverso un comportamento attivo e positivo da parte dell'interessato (considerando 32 GDPR)[52].

La disciplina generale del consenso individuale è poi rifinita da due ulteriori norme: quella che ne sancisce la natura revocabile (art. 7, par. 3, GDPR) e quella che impone al titolare del trattamento di darne prova una volta rilasciato dall'utente (art. 7, par. 1, GDPR).

Nell'ambito dell'Unione europea, le più recenti normative relative allo sviluppo delle nuove tecnologie e al trattamento dei dati ad esse correlato dedicano senz'altro meno spazio alla definizione e alla disciplina dell'assenso individualmente prestato. Tuttavia, il frequente richiamo al *General Data Protecion Regulation* in esse presente impone di considerare la logica del consenso individuale – così come emergente dal medesimo – anche in relazione alla loro applicazione[53].

Il Regolamento 2023/2854 (c.d. *Data Act*), ad esempio, subordina il trattamento dei dati relativi all'utente – soprattutto se egli è persona fisica coincidente con la figura dell'interessato, e qualora i dati siano generati dall'uso di prodotti connessi e servizi correlati – alla disciplina prevista dal GDPR (considerando 34), il quale si pone addirittura in regime di prevalenza sul predetto regolamento in caso di conflitto (art. 1, par. 5)[54]; sicché, sebbene nella presente disciplina i riferimenti all'assenso individualmente prestato siano alquanto tenui, il rinvio esplicito al Regolamento 2016/679 fa rivivere anche in tale contesto normativo le pratiche consensuali che, come si è visto, ne costituiscono un rilevante fulcro. Il Regolamento 2024/1689 (c.d. *AI Act*), invece, non solo lascia distinta e impregiudicata la regolazione del consenso individuale degli interessati al trattamento dei loro dati personali dettata nel *General Data Protecion Regulation* (considerando 141), ma ad essa assomma un'ulteriore ipotesi di assenso, quello informato, da intendersi quale "espressione libera, specifica,

51. In merito alla forma dell'informazione fornita all'interessato, l'art. 12, par. 1, GDPR precisa: "il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato".

52. Così era già stato specificato da Article 29 Data Protection Working Party 2010, p. 13. Anche la Corte di Giustizia dell'Unione europea si è pronunciata sul punto, correlando l'inequivocabilità del consenso alla sua prestazione attraverso un comportamento (materiale o verbale) positivo, attivo e deliberato dall'utente: cfr. Corte di giustizia dell'Unione europea, 1 ottobre 2019, C-673/17, *Planet49*, e Corte di giustizia dell'Unione europea, 11 novembre 2020, C-61/19, *Orange România SA* c. *Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP)*. Cfr. anche Caggiano 2017, p. 9.

53. Si ricorda, preliminarmente, che l'art. 8, par. 2, della Carta di Nizza, pur aprendo alla forza legittimante di altre e differenti basi giuridiche, dispone in via generale che il trattamento dei dati di carattere personale debba svolgersi non solo secondo i principi di lealtà e finalità determinata, ma anche nel rispetto del "consenso della persona interessata", unica condizione di legittimità espressamente menzionata dalla Carta dei Diritti Fondamentali dell'Unione europea.

54. Nel Regolamento (UE) 2023/2854, il riferimento al consenso diventa esplicito nella parte centrale del considerando 34, parte nella quale si afferma che "se l'utente non è l'interessato ma un'impresa, ivi incluso un imprenditore individuale, ma non nei casi di uso domestico condiviso del prodotto connesso, l'utente è considerato un titolare del trattamento. Di conseguenza tale utente che, in qualità di titolare del trattamento, intenda richiedere dati personali generati dall'uso di un prodotto connesso o di un servizio correlato, deve disporre di una base giuridica per il trattamento dei dati come previsto dall'articolo 6, paragrafo 1, del Regolamento (UE) 2016/679, come il consenso dell'interessato o l'esecuzione di un contratto di cui l'interessato è parte".

inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare" (art. 3, par. 1, n. 59).

L'adesione all'approccio teorico che va sotto il nome di *Individual Control Model*, peraltro, non è propria soltanto del legislatore europeo. Come osservano Daniel J. Solove e Woodrow Hartzog, infatti, "in the United States, many laws sought to implement the Individual Control Model through the notice-and-choice approach, where organizations posted notices about their privacy practices and individuals could opt out if they objected"[55].

Addirittura, dunque, in molte normative sulla privacy elaborate ed emanate da legislatori di oltreoceano non si richiede nemmeno che il consenso dell'individuo sia espresso attraverso un comportamento attivo (*opt-in*). Esso si desume sovente per *facta concludentia*, ovverosia sulla base delle condotte materialmente tenute dall'utente durante la navigazione sul web, pur potendo sempre essere revocato da quest'ultimo istantaneamente o in un momento successivo (*opt-out*)[56].

In generale, pertanto, traspare un'evidente adesione da parte dei legislatori europei e statunitensi a un modello di contrasto alla *dataveillance* e ai suoi effetti più nocivi fondato sulla libera scelta di ciascuna persona. Elargendo in gran quantità facoltà e diritti al singolo soggetto, si cerca di porre costui nella posizione ottimale per poter controllare e gestire i propri dati. Attraverso la libertà e l'informazione che dovrebbero dare fondamento a ciascun consenso rilasciato da ogni individuo, quest'ultimo dovrebbe vedere rinforzata la propria posizione nei confronti di istituzioni pubbliche e imprese private, e dovrebbe riuscire a fuoriuscire dallo stato di minorato potere a cui lo relega l'asimmetria informativa rispetto ad esse.

Tuttavia, come si evidenzierà nel paragrafo successivo, tale approccio non pare da solo sufficiente a fronteggiare i pericoli insiti in forme di monitoraggio capaci di arrecare danno non solo al soggetto ma anche alla società in cui esso vive ed opera quotidianamente.

4. Consenso senza senso

Il quadro normativo che ritrae il consenso quale prima forma di contrasto al controllo oggi reso possibile dai dispositivi tecnologici appare assai suggestivo. Esso tenta di bilanciare la perdita di potere e conoscenza generata dalla vigilanza contemporanea in capo all'individuo tramite il riconoscimento di strumenti tecnico-giuridici in grado di riaffermarne la capacità di libera autodeterminazione. Tuttavia, gli accesi e scintillanti colori di tale disegno legislativo non devono distogliere l'attenzione del critico dai limiti tecnici da cui esso è intrinsecamente affetto.

Nelle pratiche quotidiane, infatti, è estremamente raro rinvenire consensi rilasciati in adesione al *gold standard* fissato dal GDPR e dalle normative ad esso affini o ispirate.

La necessità di fondare il trattamento dei dati personali su un consenso pienamente informato e consapevole si scontra sovente con delle informative privacy assai prolisse, difficilmente intellegibili per linguaggio e riferimenti, nonché contraddistinte da un elevato grado di vaghezza[57]. Il tempo necessario alla lettura materiale delle *privacy*

55. Solove–Hartzog 2024, pp. 1025-1026. Un esempio è rappresentato dal *California Consumer Privacy Act* (CCPA), una delle prime normative complete in materia di privacy emanata negli Stati Uniti, entrata in vigore il 1° gennaio 2020 e successivamente modificata ed estesa nel 2023 dal *California Privacy Rights Act* (CPRA). In parte ispirato al GDPR, il CCPA guarda ancora con attenzione prevalente all'individuo e tende a fare affidamento perlopiù sulle sue decisioni personali quanto a tutela della riservatezza: cfr. Cal. Civ. Code § 1798.120(a).

56. Daniel J. Solove riassume efficacemente la dinamica: "organizations create a privacy notice (also called a 'privacy policy' or 'privacy statement') to inform people about the collection and processing of personal data. Individuals are given a 'choice' to opt out of certain uses and disclosures, such as sharing or selling personal data to third parties. At its most basic, the choice is take-it-or-leave-it—either do business with an organization or do not. In other instances, organizations present ways to opt out of certain data uses; if people fail to opt out, then they are deemed to consent": Solove 2024, pp. 599-600.

57. Cfr. Orefice 2018, p. 105; Custers–Dechesne–Pieters et al. 2019, p. 249; Maestri 2021, p. 69; Di Corinto 2022, p. 33; Coniglione 2023, p. 6.

policy[58] e la mancanza di conoscenze tecnico-giuridiche di base per poterle comprendere[59] – e, conseguentemente, per riuscire a prendere sulla base di esse decisioni realmente ragionate – rappresentano due ostacoli per ora ancora ampiamente insormontabili.

Peraltro, non deve dimenticarsi che le informative privacy concernono il trattamento di dati da parte di sistemi informatici in rapida e continua evoluzione. Sicché nessuna *privacy policy* può considerarsi definitiva e immutabile nel tempo[60]. Irrealisticamente, ciò comporta che a ogni (necessaria) modifica dell'informativa privacy da parte del titolare del trattamento dovrebbe seguire una comunicazione all'interessato, il quale, pur essendo spesso sprovvisto di entrambi, dovrebbe impiegare ulteriori tempo e competenze per riconsiderare un consenso già preventivamente prestato e decidere se confermarlo o no[61].

Benché numerosi siano stati i moniti della dottrina e i tentativi da parte delle autorità competenti volte a una sensibile mitigazione della complessità che caratterizza le *privacy policy*[62], ancor oggi la gran parte degli utenti risulta essere scarsamente incentivata alla lettura di informative privacy tutt'altro che accessibili[63]. Con il risultato che molte persone finiscono per acconsentire alla cessione e al trattamento dei propri dati personali senza (poter) avere la minima idea di quali siano i termini destinati a regolare tali operazioni nel caso concreto[64].

Anche la specificità del consenso pone problematiche di difficile risoluzione.

Affinché tale requisito possa dirsi pienamente integrato, è necessario che le richieste formulate all'utente siano granulari, ovverosia puntuali e circoscritte. Tuttavia, l'esigenza di specificità dell'assenso e delle domande che lo precedono rischia di avere quale unico esito la proliferazione di informative e richieste, così tecniche e numerose da non sortire alcun effetto se non quello di confondere ulteriormente l'utente[65].

Quanto alla libertà del consenso, essa è chiamata a fare i conti con il crescente valore pecuniario dei dati, i quali sono divenuti in breve tempo il nuovo oro nero nelle economie mondiali[66].

È noto, nell'ambito dei *surveillance studies*, che molti dei beni e servizi (perlopiù online) che

58. Cfr. Custers–Dechesne–Pieters et al. 2019, p. 253. Già nel 2008 Aleecia McDonald e Lorrie Cranor rilevavano che soltanto per leggere le informative privacy gli utenti avrebbero dovuto spendere 201 ore ogni anno (poco più di 8 giorni): cfr. McDonald–Cranor 2008. Recenti studi dimostrano che negli ultimi vent'anni la lunghezza media delle *privacy policy* è notevolmente aumentata, e con essa anche i tempi di lettura: cfr. Schwab 2018; Litman–Navarro,2019; Stokel–Walker 2022.
59. Cfr. Custers–Dechesne–Pieters et al. 2019, pp. 251 e 253; Solove 2021, p. 5; Solove 2024, pp. 618-619. Su pregiudizi ed errori che, più in generale, contraddistinguono le decisioni degli individui in materia di privacy e cessione dei dati cfr. Kesan–Hayes–Bashir 2016.
60. Cfr. Custers–Dechesne–Pieters et al. 2019, 251.
61. Tale dinamica, infatti, molto spesso non si verifica: cfr. Solove 2024, p. 609.
62. Sulla necessità, manifestata in dottrina, di un'informativa privacy dettagliata e completa, ma al contempo accessibile e comprensibile cfr., ad esempio, Hintze 2017; Orefice 2018, *passim*; Custers–Dechesne–Pieters et al. 2019, pp. 248-249. Tale esigenza è stata ribadita dalla giurisprudenza della Corte di Giustizia dell'Unione europea nelle sentenze: Corte di giustizia dell'Unione europea, 1 ottobre 2019, C-673/17, *Planet49*, e Corte di giustizia dell'Unione europea, 11 novembre 2020, C-61/19, *Orange România SA* c. *Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP)*. A livello normativo, l'invito a formulare informative privacy concise, comprensibili e basate su un linguaggio chiaro e semplice si rinviene, ad esempio, in: considerando 58 GDPR, e Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-574(C).
63. Cfr. Becker 2019, p. 310, Solove –Hartzog 2024, p. 1026; Solove 2024, p. 597.
64. Cfr. Solove 2024, p. 614.
65. Cfr. Solove 2024, pp. 622-623. In generale, sulla natura controproducente della prassi di fornire all'utente una quantità eccessiva di informazioni (*information overload*) cfr. Bawden–Robinson 2020.
66. Sul valore economico dei dati cfr. Orefice 2018, p. 176; Bazzoni 2019, p. 642; Lyon 2020, p. 82 ss.; Paolucci 2021, p. 207; Di Corinto 2022, p. 31.

vengono presentati come gratuiti lo sono soltanto in termini strettamente monetari. In verità, essi vengono pagati dagli utenti con una moneta molto più duttile e potenzialmente fruttuosa, ovverosia la cessione di informazioni[67].

Se tale realtà risulta essere ampiamente riconosciuta negli ambienti specialistici, non pare che al riguardo vi sia altrettanta consapevolezza in coloro che, come la maggior parte dei soggetti che conducono la loro vita nelle società contemporanee, fanno un uso quotidiano di Internet e dei dispositivi ad esso connessi. La mancanza di consapevolezza circa il valore economico dei dati personali e il loro utilizzo come merce di scambio da parte di entità pubbliche e private rende gli individui disposti a cedere a cuor leggero un'ingente quantità di informazioni, anche di molto maggiore rispetto a quella strettamente necessaria, pur di ottenere in cambio un bene o un servizio per il quale non è richiesto alcun esborso di denaro[68].

La prestazione del consenso alla cessione dei dati, dunque, non può considerarsi mai del tutto libera in quanto rappresenta frequentemente la condizione necessaria e sufficiente per poter fruire di un vantaggio che altrimenti non si potrebbe ricevere o per il quale sarebbe altresì necessario il pagamento di una somma di denaro[69].

L'assenso concretamente prestato dall'individuo risulta essere il più delle volte soltanto una "fiction", una copia sbiadita e infedele di un modello normativo di consenso tanto ideale quanto astratto, in quanto "the conditions for meaningful consent mainly exist [only] in a fairy tale"[70].

Più in generale, attraverso le loro pratiche quotidiane i soggetti dimostrano di non avere piena coscienza delle conseguenze derivanti a livello individuale e collettivo dalla cessione di ingenti quantitativi di informazioni a terzi[71].

In parte ciò è dovuto alla capacità dei programmatori di sfruttare a proprio favore il grado di irrazionalità insito in ogni decisione umana: la richiesta di consenso viene formulata all'utente secondo tempi e modalità e sulla base di *design* che lo incentivano a rispondere affermativamente (*nudge*)[72], nonché in contesti che lo inducono a sottovalutare la portata delle scelte che sta compiendo (*gamification*)[73]. D'altro canto, è chiaro che i benefici derivanti dalla prestazione del consenso risultano essere, agli occhi dell'utente, ben più tangibili e immediati dei pericoli connessi alla cessione dei dati, i quali si palesano soltanto come un'ombra remota e indeterminata[74].

Dunque, benché in generale le persone affermino di avere un'alta considerazione della riservatezza e di avere a cuore la sua tutela, in concreto esse non paiono particolarmente preoccupate dei rischi annessi alla cessione di dati personali a entità pubbliche e private. Nondimeno, esse non esitano a riporre informazioni personali nelle mani di terzi, anche a fronte di vantaggi estremamente esigui, e

67. Sulla presunta gratuità di beni e servizi che, in realtà, vengono "pagati" dall'utente attraverso la cessione dei suoi dati personali cfr. Delmastro–Nicita 2019, pp. 24-25; Fioriglio 2021, p. 89; Battelli 2022, p. 355; Di Corinto 2022, p. 33; Ferraris–Saracco 2023, pp. 57-58; Pietrangelo 2023, p. 939; Capilli 2024, p. 3.

68. Cfr. Greenfield 2017, p. 28; Delmastro–Nicita 2019, p. 43; Perri 2020, pp. 13-14; Di Corinto 2022, *passim*, Coniglione 2023, p. 2.

69. Cfr. Orefice 2018, pp. 110-113; Custers–Dechesne–Pieters et al. 2019, p. 253; Solove 2021, p. 36; Solove 2024, p. 607.

70. Solove 2024, p. 596. Cfr. anche Pin 2021, p. 48.

71. Cfr. Sarra 2024, p. 11.

72. Cfr. Hartzog 2018-a, pp. 427-428; Hartzog 2018-b, pp. 21-23; Mathur–Acar–Friedman et al. 2019; Waldman 2020, p. 105; Solove 2021, p. 21.

73. Sul modo, appunto, giocoso con cui la dimensione digitale viene presentata e accolta anche in riferimento alla privacy cfr. Greenfield 2017, p. 34; Delmastro–Nicita 2019, p. 105; Maestri 2021, p. 62; Han 2022, p. 16; Han 2023, p. 20.

74. Sulla difficoltà degli individui di considerare correttamente i possibili rischi derivanti dalle decisioni assunte in un contesto complesso e sulla tendenza a cogliere perlopiù i vantaggi immediati anziché i costi di lungo termine cfr., quale studio autorevole, Acquisti–Grossklags 2004, pp. 172–173. Cfr. anche Solove 2021, pp. 19 e 43-44, e Solove 2024, p. 620.

non sono disposte a investire denaro per salvaguardare la propria riservatezza[75]. Tale fenomeno risulta essere talmente diffuso e scientificamente comprovato da aver assunto, a partire dal 2007, la denominazione di *privacy paradox*[76]. Non v'è dunque da meravigliarsi se "surveillance isn't just hoisted upon people; many people eagerly sign up for it […] embrace and normalize the fruits of the digital age, no matter how poisonous they might be [and] will often make choices that are not in their own best interest"[77].

Il progresso tecnologico, a sua volta, non ha favorito la salubrità della pratica del consenso.

In un mondo dove la Rete è diventata il principale mezzo per svolgere attività individuali e collettive, l'individuo viene insistentemente sommerso da richieste di assenso, le quali, pertanto, vengono percepite più come un noioso impiccio del quale sbarazzarsi al più presto anziché come un utile strumento con il quale potersi difendere da indebite invasioni della propria sfera privata (*consent fatigue*)[78]. Senza dimenticare il fatto che con l'avvento dell'*Internet of Things* ogni persona si ritrova quotidianamente circondata da dispositivi che raccolgono dati senza che ciò avvenga necessariamente sulla base di un preventivo consenso[79].

Per quanto vaste siano, poi, le possibilità di scelta messe a disposizione dell'utente circa la cessione dei propri dati, esse saranno sempre limitate e predeterminate da parte dei programmatori, sicché non sarà mai possibile una reale personalizzazione della quantità di dati trasmessi e delle modalità della loro cessione[80].

In definitiva, il consenso non pare poter rappresentare uno strumento da solo capace di permettere all'individuo di fronteggiare le molteplici insidie lanciate dalle odierne forme di monitoraggio. I rilevanti pericoli per i soggetti e per la società passibili di essere creati dalla sorveglianza contemporanea difficilmente possono essere fronteggiati attraverso un assenso sbrigativamente prestato da una persona condizionata nelle sue decisioni e incapace di avere piena contezza delle conseguenze delle sue scelte.

Applicato nei termini anzidetti, il consenso rischia di essere non tanto uno scudo a difesa degli individui e delle comunità che essi compongono, bensì una spada con la quale entità pubbliche e private possono più agevolmente penetrare laddove si annidano i dati di cui necessitano per trarre profitto.

5. Agire, ma in quale direzione?

I rischi individuali e collettivi connessi alla sorveglianza in generale e alle odierne forme di monitoraggio in particolar modo non possono essere negati, né tantomeno possono essere svalutati o dimenticati.

I pericoli derivanti dalla trasparenza totale dei soggetti e dalla loro reclusione all'interno di *echo*

75. Cfr. Barth–De Jong–Junger et al. 2019. Cfr. anche Solove 2021, p. 21.
76. Cfr. Norberg–Horne–Horne 2007. Benché sia assodato in letteratura il fatto che sovente gli individui non siano coscienti dei rischi a cui la collettività e loro stessi si espongono attraverso la cessione dei dati, e che, in ogni caso, tali pericoli siano oggetto di una generale sottovalutazione, vale la pena ricordare che il concetto di *privacy paradox* non è del tutto pacifico in dottrina. Daniel J. Solove osserva al riguardo: "because behaviour and attitudes regarding privacy are about different things, the fact that they do not align is not a discrepancy. It is not even clear that they can be brought into alignment. Depending upon which side one takes, it can be tempting to view behaviour or attitudes as a more fixed reflection of people's true preferences, with the other being false or skewed. But behaviour and attitudes are highly malleable and are quite different. Behavior involves risk decisions within specific contexts; it is always context dependent. Attitudes are more general views about value and can exist beyond specific contexts. The fact that attitudes and behaviour about privacy diverge is not a paradox or even an inconsistency": Solove 2021, p. 4.
77. Solove–Hartzog 2024, p. 1032.
78. Cfr. Hartzog 2018-a, p. 429, Custers–Dechesne–Pieters et al. 2019, pp. 247 e 253; Solove 2021, p. 45; Solove 2024, p. 597. Per una panoramica del numero di richieste di consenso ricevute mediamente da un utente cfr. Olmstead–Atkinson 2015.
79. Cfr. Hartzog 2018-a, pp. 429-430. Sul funzionamento dell'IoT cfr. Greenfield 2017, p. 32 ss.
80. Cfr. Hartzog 2018-a, pp. 426-427.

chambers costituite da dati suggeriscono, al contrario, di trattare della sorveglianza attuale con ancora maggior impegno. I valori umani e sociali in gioco allorquando ci si occupa di privacy devono ritenersi talmente rilevanti e meritevoli di tutela da imporre a tutti i *surveillance scholars* di occuparsene, rimanendo aperti alla possibilità di sondare anche orizzonti finora ignorati o sottovalutati.

Oggigiorno numerose sono le persone, soprattutto di giovane età, che ritengono inutile e velleitario qualsivoglia tentativo di proteggere la propria sfera privata, di controllare le informazioni personali o di prevenire i rischi connessi alle dinamiche di controllo, stante l'ubiquità e la potenza tecnologica dei dispositivi attraverso i quali avviene il trattamento dei dati[81]. Tuttavia, dinanzi a uno scenario tutt'altro che incoraggiante, abbandonarsi all'inevitabilismo appare una soluzione tutt'altro che auspicabile[82]. L'attuale incapacità dell'individuo di fronteggiare i rischi collegati alla sorveglianza tramite i mezzi oggigiorno messigli a disposizione dal legislatore deve essere un incentivo a immaginare strumenti migliori e più efficaci, non una comoda giustificazione per rassegnarsi e disinteressarsi della questione.

D'altro canto, deve ritenersi altrettanto irragionevole l'ipotesi di un atteggiamento totalmente avverso alle odierne forme di vigilanza. Per quanto inquietanti possano essere alcune delle sue derive, infatti, la sorveglianza presenta anche profili positivi meritevoli, per ciò stesso, di essere conservati e valorizzati[83].

In questi termini appare condivisibile la posizione assunta da Daniel J. Solove, secondo il quale "privacy will not always win out"[84]. Le prospettive che parlano delle forme di monitoraggio presentandole perlopiù come un "nemico"[85] o un "avversario"[86] da annientare *in toto* danno prova del loro carattere deficitario, incurante cioè della necessità di preservare talvolta anche la sorveglianza stessa, sebbene ciò implichi una qualche compressione della riservatezza. In altri termini, una teorizzazione finalizzata all'integrale tutela della privacy attraverso la completa eliminazione di qualsivoglia dinamica di controllo rischia di provocare più pregiudizi di quelli che essa intenderebbe rimuovere.

Qualunque sia la possibile soluzione al problema, dunque, essa non potrà che implicare un bilanciamento tra i molteplici valori e interessi in gioco. Quale direzione intraprendere, però, per raggiungere tale equilibrio?

Fare affidamento perlopiù sulla responsabilità dei *big players* e dei loro programmatori appare una prospettiva utile ma tutt'altro che risolutiva.

Innanzitutto, anche ammessa la buona fede delle *big tech*, non sembra logico e realistico credere che la tutela della privacy degli utenti possa essere garantita *in toto* proprio da coloro che più di tutti hanno interesse (economico) allo svelamento della sfera privata degli individui. Successivamente, è necessario evidenziare che i sistemi di *privacy by design* e *privacy by default* elaborati dai programmatori dei *big players* medesimi (anonimizzazione e crittografia su tutti) non possono dirsi del tutto affidabili nella protezione della riservatezza[87].

81. Cfr. Hargittai–Marwick 2016; Hoffmann–Lutz–Ranzini 2016; Solove 2021, pp. 45-46; Maestri 2021, p. 58.
82. Sulla tendenza a considerare la computazione ubiqua e la sorveglianza come fenomeni inarrestabili, passibili soltanto di essere accettati cfr. Zuboff 2019, p. 236.
83. Se, infatti, è innegabile che la *surveillance* rivesta oggi un ruolo di rilievo nella deterrenza e, soprattutto, nella repressione della criminalità, non va dimenticato che è la *dataveillance* a rendere possibili molte delle amenità di cui attualmente è possibile godere, nonché a permettere il buon funzionamento di dispositivi oggi ritenuti essenziali in molteplici contesti.
84. Solove 2021, p. 38.
85. Zuboff 2019, pp. 295-296.
86. Brunton–Nissenbaum 2016, p. 20.
87. Da un lato, la pratica dell'anonimizzazione delle informazioni è resa inefficace dall'alto numero di dati e metadati che ciascun individuo rilascia nel corso della sua routine quotidiana: cfr. Custers–Dechesne–Pieters et al. 2019, p. 255. Anche la crittografia non garantisce una sicurezza assoluta in quanto è possibile, sebbene talvolta con una certa complessità, ricostruire algoritmicamente il testo in chiaro a partire da quello cifrato: cfr. Perri

Del pari, però, non sembra opportuno proseguire esclusivamente sulla via tracciata negli ultimi decenni dai principali legislatori del mondo. E ciò non solo in virtù della natura sfuggente del consenso[88] e delle molteplici problematiche irrisolte messe in luce nel paragrafo precedente.

Come evidenziano Daniel J. Solove e Woodrow Hartzog, insistere su un approccio normativo fondato in via esclusiva sull'*Individual Control Model* appare non solo inutile ma addirittura controproducente[89].

Da un lato, infatti, riconoscere all'individuo facoltà e diritti estremamente rilevanti sulla carta, ma difficilmente esercitabili e scarsamente influenti in concreto, alimenta nei soggetti un senso di controllo sui propri dati che tuttavia è soltanto illusorio[90]. Accreditare ulteriori libertà formali incapaci, però, di garantire una tutela effettiva della privacy altro non permetterebbe se non di far abbassare la guardia alle persone, agevolando così le attività di trattamento dei dati da parte di chi ve ne ha interesse[91].

Dall'altro lato, continuare a fare affidamento prevalentemente su un assenso dato troppo spesso con eccessiva facilità rischia di far ricadere la responsabilità circa gli effetti negativi della sorveglianza sugli utenti stessi. Se, infatti, la normativa vigente ritiene sufficiente il consenso per poter considerare legittimi i trattamenti dei dati, allora a titolari e responsabili degli stessi basterà riuscire ad ottenere formalmente quest'ultimo, indipendentemente dal fatto che esso sia frutto di un ragionamento consapevole o della pura e semplice volontà di sbarazzarsi quanto prima di un "fastidioso" *banner*. Sicché, qualora successivamente emergano delle conseguenze nocive a partire dalla cessione di dati, la responsabilità dovrà riconoscersi non tanto su quanti li hanno trattati a norma di legge, quanto piuttosto in capo a coloro che hanno legittimato il trattamento attraverso il loro assenso[92].

In generale, e alla luce dei più autorevoli studi comportamentali in ambito psicologico e antropologico succedutisi negli ultimi cinquant'anni, sembra quantomeno inopportuno proseguire in una direzione volta prevalentemente all'eccessiva esaltazione del ruolo dell'individuo e delle sue decisioni personali.

Nella seconda metà del secolo scorso, Daniel Kahneman e Amos Tversky sconfessarono l'allora tradizionale e consolidato filone di pensiero che raffigurava l'essere umano come un *homo oeconomicus* perfettamente razionale nelle sue scelte, soprattutto in ambito economico: essi, infatti, dimostrarono che è assai frequente che, nelle pratiche negoziali e di scambio in particolare, i soggetti cadano vittime di molteplici errori provocati perlopiù da euristiche e distorsioni cognitive[93].

2020, p. 108. Per titolari e responsabili del trattamento anche l'obbligo di provvedere alla cancellazione dei dati personali di un utente dietro richiesta esplicita di quest'ultimo potrebbe non essere sempre agevole o potrebbe essere addirittura inefficace, posto che il carattere aperto dell'architettura di Internet mina ampiamente la capacità di controllare i flussi di dati: cfr. Custers–Dechesne–Pieters et al. 2019, p. 252. In generale, poi, va evidenziato che il funzionamento degli algoritmi risulta essere così opaco da non (poter) essere del tutto chiaro nemmeno per le imprese che se ne servono: cfr. Maestri 2021, p. 61; Varoufakis 2023, p. 117; Pietropaoli 2024, *passim*.

88. Sulla difficoltà di stabilire in concreto quando il consenso prestato da un utente possa dirsi realmente rispettoso del *gold standard* preteso dalla maggior parte dei legislatori mondiali cfr. Custers–Dechesne–Pieters et al. 2019, p. 250.

89. Cfr. Solove–Hartzog 2024, pp. 1023-1024 e Solove 2024, p. 596.

90. Cfr. Hartzog 2018-a, pp. 425-426; Solove 2021, pp. 5-6; Solove–Hartzog 2024, pp. 1031-1032 e 1036.

91. Come evidenzia Woodrow Hartzog, "the problem with respecting everyone's personal commitments is that for-profit tech companies have their own agendas. They want users to be maximally forthcoming to monetise all this information. Hence, it is to their advantage to make users believe they have more control than they are actually given": Hartzog 2018-a, p. 426. Tra gli studi più autorevoli in materia cfr. Brandimarte–Acquisti–Loewenstein 2013.

92. Cfr. Solove–Hartzog 2024, p. 1036.

93. Cfr. Kahneman–Tversky 1979. Ben più di recente, Richard H. Thaler e Cass R. Sunstein, nell'ambito dei loro studi congiunti in tema di *nudge*, hanno ripreso e approfondito ulteriormente le rivoluzionarie teorie dei due

Se, dunque, le persone si rendono quotidianamente protagoniste di scelte che, per quanto banali possano essere, si rivelano sovente irrazionali e, talvolta, addirittura nocive per se stesse, è alquanto insensato credere che una simile inclinazione naturale possa trovare redenzione in un contesto estremamente articolato quale quello della *privacy online*. Prendere una decisione razionale e per sé vantaggiosa non è agevole, nemmeno in ambiti di cui gli esseri umani hanno da sempre esperienza materiale; *a fortiori* tale operazione è destinata a essere ben più ardua in un contesto molto meno concreto, ben più ambiguo e assai meno conosciuto come quello della riservatezza, peraltro nell'articolata dimensione digitale e interconnessa[94].

Con ciò non si desidera affatto affermare la necessità di sottrarre agli individui la loro libertà di scelta, né privarli *in toto* della loro facoltà di esprimere opinioni e assensi. Al contrario.

Come osserva opportunamente Stacy-Ann Elvy, "if consent is used to justify data practices, consent should be meaningfully and validly obtained […]"[95]. Tuttavia, come anzidetto, le prassi individuali e le ricerche scientifiche invalse negli ultimi decenni dimostrano inconfutabilmente che il consenso perfettamente aderente al *gold standard* legislativo rappresenta più una lontana chimera che una realtà concreta, sicché può dirsi pervenuto il momento di abbandonare almeno in parte la logica dell'assenso, proprio in quanto incapace, da sola, di assicurare effettività alle decisioni individuali e garantire una tutela piena della privacy. È necessario, cioè, prendere atto della natura *murky* del consenso individuale[96] allo scopo di pianificare soluzioni che consentano di sopperire al suo carattere deficitario.

L'obiettivo, pertanto, è quello di proporre modelli che permettano di istaurare contesti giuridico-sociali ove le scelte dei soggetti possano essere davvero consapevoli e, dunque, realmente incidenti sul trattamento dei dati, senza per ciò stesso dover rinunciare ai vantaggi garantiti dalla sorveglianza.

6. Una prospettiva per il futuro: il *Societal Structure Model*

Nelle sue condizioni attuali, l'individuo non può dirsi in grado di fronteggiare, da solo, le molteplici dinamiche che attentano quotidianamente alla sua sfera privata[97].

Poiché, tuttavia, le misure predisposte finora dai principali legislatori mondiali non hanno sortito appieno gli effetti di *empowerment* che ci si attendeva da esse, sembra opportuno iniziare a porre lo sguardo su soluzioni ancor oggi scarsamente battute a livello normativo, ancorché da tempo caldeggiate, nell'ambito dei *surveillance studies*, da una rilevante componente della dottrina.

Ciò che appare innanzitutto fondamentale è l'istruzione[98].

Il mondo digitale in cui siamo chiamati a vivere e operare quotidianamente offre una quantità di vantaggi e opportunità senza precedenti. Tuttavia, esso risulta essere foriero di rischi altrettanto

psicologi israeliani, affermando che "le previsioni degli esseri umani sono imprecise e distorte" e che "anche il loro processo decisionale presenta numerosi difetti": cfr. Thaler–Sunstein 2014, p. 14. Per un'analisi recente dei principali *bias* incidenti sulle decisioni delle persone in ambito negoziale cfr. Antonazzi 2020.

94. Senza, peraltro, dimenticare che le scelte compiute in materia di privacy da un singolo soggetto possono produrre i propri effetti pratici anche nei confronti di altri individui, assumendo così una dimensione inevitabilmente collettiva. Come Custers e colleghi notano, "the use of Big Data increasingly enables the prediction of characteristics of people who withheld consent on the basis of the information available from people who did consent. When large numbers of people consent to the use of their personal data, it is possible to predict missing values of other people": Custers–Dechesne–Pieters et al. 2019, p. 252.

95. Elvy 2024, p. 644.

96. Sul concetto di *murky consent* cfr. Solove 2024.

97. Sulla vulnerabilità dell'individuo e sulla sua incapacità attuale di reagire da solo alle sfide della sorveglianza contemporanea cfr. Seminara 2018, p. 134, e Zuboff 2019, p. 238.

98. Sull'importanza dell'educazione dell'utente con particolare riferimento alla privacy cfr. Weinberger–Bouhnik–Zhitomirsky-Geffet 2017; Custers–Dechesne–Pieters et al. 2019, p. 255; Pietropaoli 2024, p. 7; Marchesin 2024-a, p. 57.

numerosi e ingenti, ancor più alti proprio perché provenienti da una dimensione intangibile, ubiquitaria e nella quale operano milioni di individui e algoritmi provenienti da ogni parte del globo. Educare al buon utilizzo dei dispositivi tecnologici di uso quotidiano e alla tutela dai pericoli individuali e collettivi che essi necessariamente implicano dovrebbe, pertanto, rappresentare un punto nodale delle politiche di istruzione, un obiettivo minimo che le istituzioni pubbliche potrebbero perseguire anche con la collaborazione di *big tech* e imprese private[99].

Proprio in virtù dei rischi enucleati nei paragrafi precedenti, educare alla tecnologia e alla dimensione digitale dovrebbe implicare anche l'erogazione di un'istruzione di base in tema di privacy.

Nel contesto attuale, dominato dalle richieste di assenso e dal valore legittimante di quest'ultimo, non è pensabile che il soggetto possa approcciare una privacy policy o assumere una decisione cosciente in merito alla cessione di informazioni personali senza avere nel proprio bagaglio culturale delle nozioni elementari concernenti la sorveglianza online, la protezione della riservatezza e il trattamento dei dati. Anche a seguito di un (auspicabile) mutamento di paradigma, tale istruzione si renderebbe comunque fondamentale: essa, infatti, andrebbe in ogni caso a sorreggere un consenso dal quale non è possibile né opportuno prescindere del tutto, e fungerebbe da sostegno per una partecipazione alla difesa della privacy da parte delle persone che si rende pur sempre essenziale.

L'educazione in materia di riservatezza appare tanto più necessaria quanto maggiori sono i valori privati e pubblici che ad essa si accompagnano[100]. In altri termini, fornire un'istruzione basilare relativamente alla privacy non significa soltanto insegnare a leggere correttamente un'informativa privacy o a utilizzare i comandi delle impostazioni delle *app* in maniera adeguata: significa porre le basi per incoraggiare una cittadinanza attiva, consapevole, libera di autodeterminarsi e propensa al dialogo e alla pacifica convivenza.

Per quanto possa essere utile, l'educazione ai media digitali e alla riservatezza che essi chiamano inevitabilmente in gioco non può considerarsi tuttavia sufficiente[101]. Affinché si verifichi un apprezzabile miglioramento nella salvaguardia della privacy e nel suo bilanciamento con altri valori ritenuti imprescindibili, si rende necessario un (quantomeno parziale) mutamento di paradigma.

Come evidenziato da numerosi *surveillance scholars*, la riservatezza costituisce un valore indispensabile non solo per l'individuo ma anche per la società intera, soprattutto se ispirata a principi democratici. Sicché è astrattamente illogico – oltre che concretamente inefficacie, come dimostrato ampiamente dalla prassi diffusa – pensare che la tutela di un diritto sia individuale che collettivo possa passare esclusivamente per le mani di soggetti singolarmente considerati[102]. Se la sorveglianza

99. In generale, il rapporto DESI (*Digital Economy and Society Index*) del 2022 testimonia che, in Italia, soltanto il 46% della popolazione possiede competenze digitali di base, denotando, così, un deficit conoscitivo anche in merito alle principali problematiche connesse alla dimensione tecnologica, privacy inclusa. Come sottolinea Giovanni Ziccardi, riservatezza e *data protection*, unitamente all'intelligenza artificiale, "non sono solo ambiti di studio prettamente tecnici, ma sono strettamente connessi alla cultura, all'essere umano, alla società in cui vive e ai grandi valori giuridici, sociali ed etici del nostro tempo", sicché il loro studio andrebbe incentivato nelle scuole di ogni ordine e grado. Lo stesso legislatore europeo sembra aver compreso la necessità di garantire una maggiore alfabetizzazione digitale, come dimostrato dall'art. 4 del Regolamento sull'Intelligenza Artificiale (Regolamento 2024/1689) entrato in vigore il 1° agosto 2024.

100. Come evidenzia Daniel J. Solove, numerosi sono i valori connessi al concetto di privacy: dalla libertà di pensiero ed espressione alla partecipazione politica, dalla facoltà di autodeterminare il proprio orientamento sessuale al diritto di aderire a un credo religioso. Cfr. Solove 2021, pp. 39-41.

101. Sebbene dipinga un quadro forse sin troppo negativo al riguardo, Daniel J. Solove sottolinea tutti i limiti di un'eventuale educazione degli utenti in materia di privacy, dall'eccessiva complessità della materia all'incapacità delle persone di tradurre in pratica quanto acquisito in linea teorica: cfr. Solove 2024, pp. 617-621.

102. Sulla privacy come valore sociale e non solo come interesse individuale cfr. Orefice 2018, p. 81; Hartzog 2018-a, pp. 430-431; Tufekci 2018; Solove 2021, pp. 5 e 34; Gandy Jr. 2021; Meneghetti 2021, p. 277; Solove–Hartzog 2024, p. 1026; Solove 2024, p. 636.

rappresenta, per taluni aspetti, una minaccia non solo per la libertà della persona ma anche per la democraticità della comunità, è necessario che la risposta alle attuali forme di monitoraggio assuma una sembianza non tanto o non solo individualistica, ma anche e soprattutto collettivistica. È auspicabile, cioè, un progressivo – anche se non definitivo – allontanamento dall'*Individual Control Model* oggi preponderante, in vista di un graduale avvicinamento a ciò che in letteratura viene definito *Societal Structure Model*[103].

Nel 2018, Max Schremes ha trasformato *None of Your Business (noyb)*, l'organizzazione *no profit* di cui è leader, in una piattaforma online avente lo scopo di "to strengthen your right to privacy". Tale obiettivo è perseguito vigilando sulla corretta applicazione delle normative in materia di sorveglianza e riservatezza da parte delle imprese private che sono tenute alla loro osservanza. Ora tramite attività di divulgazione online, ora attraverso la predisposizione di progetti e standard da sottoporre al vaglio dei legislatori europei, ora facendo in modo di "to submit data protection complaints with local authorities and file procedures in national courts", *noyb* mira a essere un punto di riferimento per gli utenti europei e non solo, nonché a garantire un controllo generale su titolari e responsabili del trattamento dei dati[104].

Benché abbia natura privatistica, *noyb* è emblema di una tipologia di piattaforme che possono rappresentare una prima fonte di ispirazione per immaginare una reazione partecipata e collettivistica alle sfide imposte dalle odierne forme di vigilanza. Essa permette di ipotizzare l'esistenza, accanto alle autorità garanti e alla figura del *Data protection officer* (DPO)[105], di un sistema istituzionalizzato che funga da raccordo tra utenti, autorità pubbliche e imprese private. Tali istituzioni intermedie non solo garantirebbero una risposta giudiziaria alle violazioni delle normative in materia di privacy da parte delle *big tech*, ma, prima ancora, assicurerebbero all'utente la possibilità di vigilare sul loro operato in merito al trattamento dei suoi dati attraverso professionisti a ciò preposti, ovvero in prima persona ogniqualvolta lo ritenesse necessario[106].

Sebbene quella delle piattaforme ed istituzioni intermedie sia, ad oggi, soltanto un'idea embrionale, essa certifica l'esigenza di un modello di tutela della riservatezza, e di contrasto agli effetti pregiudizievoli della sorveglianza, che si fondi non più sul debole consenso dell'individuo ma sulla forte partecipazione collettiva di tutti i componenti delle società interessate da tale fenomeno. In altri termini, affinché sia possibile iniziare a immaginare un monitoraggio rispettoso degli ideali democratici e delle persone che concretamente vivono nelle odierne democrazie, è necessario cominciare a ipotizzare e progettare un movimento che prenda le mosse dallo stesso *demos*.

Riferimenti bibliografici

A. Acquisti, J. Grossklags (2004), *Privacy Attitudes and Privacy Behavior. Losses, Gains, and Hyperbolic Discounting*, in "Economics of information security", vol. 12, 2004

103. Sulla necessità di un mutamento di paradigma che, accanto alla libertà di scelta degli individui, preveda la possibilità per i funzionari pubblici di selezionare preventivamente le pratiche da ritenersi sicure per le persone e coerenti con i principi giuridici vigenti cfr. Hirsch 2020.

104. Tutte le informazioni relative al funzionamento e alle attività di *noyb* sono consultabili sul sito.

105. Per Daniel J. Solove, il ruolo dei DPO dovrebbe essere comunque implementato da parte dei legislatori: cfr. Solove 2021, p. 50.

106. Tale ipotesi appare coerente con la prospettiva di stampo sindacalistico caldeggiata da Shoshana Zuboff, secondo la quale, "per quanto possa essere determinato, un individuo isolato non può sostenere il peso della giustizia, così come un singolo lavoratore all'inizio del Ventesimo secolo non poteva combattere da solo per uno stipendio equo e il miglioramento delle condizioni in fabbrica. All'epoca fu necessaria un'azione collettiva, e lo stesso vale oggi. […] Un secolo fa, i lavoratori si organizzarono collettivamente e guadagnarono potere, e allo stesso modo oggi gli utenti si devono mobilitare secondo le 'condizioni d'esistenza' del Ventunesimo secolo. […] Ci vuole un'azione collettiva per imporre finalmente leggi che stabiliscano il diritto al santuario e al futuro come condizioni essenziali per una vita degna": Zuboff 2019, pp. 500-501.

M. Antonazzi (2020), *La negoziazione cognitiva*, in C. Sarra, F. Reggio (a cura di), "Diritto, metodologia giuridica e composizione del conflitto", Primiceri Editore, 2020

Article 29 Data Protection Working Party (2010), *Parere 2/2010 sulla pubblicità comportamentale online*, WP 171, 2010

S. Barth, M.D.T. De Jong, M. Junger et al. (2019), *Putting the Privacy Paradox to the Test. Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources*, in "Telematics and Informatics", vol. 41, 2019

E. Battelli (2022), *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono "gratuiti"*, in "I Contratti", 2022, n. 3

G. Bazzoni (2019), *La libertà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei global social media*, in "Diritto di Internet", 2019, n. 4

D. Bawden, L. Robinson (2020), *Information Overload: An Overview*, in "Oxford Encyclopedia of Political Decision Making", Oxford University Press, 2020

M. Becker (2019), *Privacy in the Digital Age. Comparing and Contrasting Individual versus Social Approaches towards Privacy*, in "Ethics and Information Technology", vol. 21, 2019, n. 4

L. Brandimarte, A. Acquisti, G. Loewenstein (2013), *Misplaced Confidences: Privacy and the Control Paradox*, in "Social Psychological and Personality Science", vol. 4, 2013, n. 3

F. Bravo (2017), *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

F. Brunton, H. Nissenbaum (2016), *Offuscamento. Manuale di difesa della privacy e della protesta*, Eretica Speciale, 2016

F. Caggia (2019), *Il consenso al trattamento dei dati personali nel diritto europeo*, in "Rivista del Diritto commerciale e del Diritto generale delle obbligazioni", 2019, n. 3

I.A. Caggiano (2017), *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in "Diritto Mercato Tecnologia", 2017

G. Capilli (2024), *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in "MediaLaws", 2024, n. 1

R. Clarke (1998), *Information Technology and Dataveillance*, Communications of ACM, 1998

C. Coniglione (2023), *L'utilizzo dei big data in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa*, in "Nomos. Le attualità nel diritto", 2023, n. 1

C. Cossutta, A. Mainardi (2018), *Sorveglianza, soggettività e spazio pubblico*, in C. Cossutta, V. Greco, A. Mainardi, S. Voli (a cura di), "Smagliature digitali. Corpi, generi e tecnologie", Agenzia X, 2018

B. Custers, F. Dechesne, W. Pieters et al. (2019), *Consent and privacy*, eLaw Working Paper Series, 2018/008, 2019

D. De Kerckhove (2016), *La rete ci renderà stupidi?*, Castelvecchi, 2016

M. Delmastro, A. Nicita (2019), *Big data. Come stanno cambiando il nostro mondo*, il Mulino, 2019

A. Di Corinto (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1

C. Doctorow (2024), *Come distruggere il capitalismo della sorveglianza*, Mimesis, 2024

S.-A. Elvy (2024), *Privacy Law Consent Conundrum*, in "Boston University Law Review", vol. 104, 2024, n. 641

M. Ferraris, G. Saracco (2023), *Tecnosofia. Tecnologia e umanesimo per una scienza nuova*, Laterza, 2023

G. Fioriglio (2021), *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in "Journal of Ethics and Legal Technologies", vol. 3, 2021, n. 2

L. Floridi (2020), *Il verde e il blu*, Raffaello Cortina Editore, 2020

O.H. Gandy Jr. (2021), *The Panoptic Sort. A Political Economy Of Personal Information*, Oxford University Press, 2021

A.M. Garofalo (2021), *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in S. Orlando, G. Capaldo (a cura di), "Annuario 2021. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università Editrice, 2021

A. Greenfield (2017), *Tecnologie radicali. Il progetto della vita quotidiana*, Einaudi, 2017

B.-C. Han (2023), *Infocrazia. Le nostre vite manipolate dalla rete*, Einaudi, 2023

B.-C. Han (2022), *Le non cose. Come abbiamo smesso di vivere il reale*, Einaudi, 2022

B.-C. Han (2021), *La società senza dolore. Perché abbiamo bandito la sofferenza dalle nostre vite*, Einaudi, 2021

E. Hargittai, A. Marwick (2016), *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy*, in "International Journal of Communication", vol. 10, 2016

W. Hartzog (2018-a), *The Case Against Idealising Control*, in "European Data Protection Law Review", 2018, n. 4

W. Hartzog (2018-b), *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, 2018

M. Hintze (2017), *In Defense of the Long Privacy Statement*, in "Maryland Law Review", vol. 76, 2017

D.D. Hirsch (2020), *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, in "Maryland Law Review", vol. 79, 2020, n. 2

C.P. Hoffmann, C. Lutz, G. Ranzini (2016), *Privacy Cynicism: A new Approach to the Privacy Paradox*, in "Cyberpsychology: Journal of Psychosocial Research on Cyberspace", vol. 10, 2016, n. 4

D. Kahneman, A. Tversky (1979), *Prospect theory: An analysis of decision under risk*, in "Econometrica", vol. 47, 1979, n. 2

J.P. Kesan, C.M. Hayes, M.N. Bashir (2016), *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, in "Indiana Law Journal", vol. 91, 2016

M. Kienke (2023), *Out of the bubble! Le tecnologie digitali e la politica del futuro*, in "Prospettiva Persona · Prospettiva Civitas", 2023, n. 2

H. Koskela (2000), *'The gaze without eyes': video-surveillance and the changing nature of urban space*, in "Progress in Human Geography", vol. 24, 2000, n. 2

K. Litman-Navarro (2019), *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, in "New York Times", 2019

D. Lyon (2020), *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, 2020

E. Maestri (2021), *Surveillance And Profiling. Online Person's Privacy Between Criminogenic Structures And Legal Paternalism*, in "Journal of Ethics and Legal Technologies", vol. 3, 2021, n. 2

L. Marchesin (2024-a), *L'eredità di Bentham. La sorveglianza post-moderna al cospetto del Panopticon*, in "Journal of Ethics and Legal Technologies", vol. 6, 2024, n. 1

L. Marchesin (2024-b), *One ring to reify them all, one ring to humanize them all. When the human eyes of restorative justice meet the dehumanizing gaze of panoptic surveillance*, in "Mediares", 2024, n. 1

A. Mathur, G. Acar, M.J. Friedman et al. (2019), *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, in "Proceedings of the ACM on Human-Computer Interaction", vol. 3, 2019

A.M. McDonald, L.F. Cranor (2008), *The Cost of Reading Privacy Policies*, in "I/S: A Journal of Law and Policy for the Information Society", vol. 4, 2008, n. 3

M.C. Meneghetti (2021), *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in "MediaLaws", 2021, n. 1

P. Moro, B. Fioravanzi (2022), *Verità digitale. Dalle fake news all'alfabetismo informativo*, in "Calumet", 2022, n. 15

P.A. Norberg, D.R. Horne, D.A. Horne (2007), *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, in "Journal of Consumer Affairs", vol. 41, 2007, n. 1

K. Olmstead, M. Atkinson (2015), *Apps Permissions in the Google Play Store*, in "Pew Research Center", 2015

M. Orefice (2018), *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne editrice, 2018

F. Paolucci (2021), *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in "MediaLaws", 2021, n. 1

E. Pariser (2012), *The filter bubble. What the Internet is Hiding from You*, Penguin Book Ltd, 2012

P. Perri (2020), *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè Francis Lefebvre, 2020

M. Pietrangelo (2023), *Spazio digitale e modelli di regolazione*, in "Consulta Online", 2023, n. 3

S. Pietropaoli (2024), *Dalla sorveglianza al controllo: la parabola della governamentalità algoritmica*, in "Rivista italiana di informatica e diritto", 2024, n. 2

A. Pin (2021), *Diritti costituzionali e intelligenza artificiale*, in P. Moro (a cura di), "Etica, diritto e tecnologia, percorsi dell'informatica giuridica contemporanea", Franco Angeli, 2021

A. Pin (2022), *Nella Rete, anche se Offline. Il ruolo dello spazio pubblico nell'era digitale*, in "Mondo Digitale", vol. 98, 2022, n. 1

D. Poletti (2019), *Le condizioni di liceità del trattamento dei dati personali*, in "Giurisprudenza italiana", 2019, n. 12

A. Purpura (2022), *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*, in "Jus Civile", 2022, n. 4

N.M. Richards, W. Hartzog (2019), *The Pathologies of Digital Consent*, in "Washington University Law Review", vol. 96, 2019, n. 6

S. Rodotà (2004), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, 2004

C. Sarra (2024), *La datificazione della persona nella costruzione del Metaverso*, in "Journal of Ethics and Legal Technologies", vol. 6, 2024, n. 1

C. Sarra (2022-a), *Il mondo-dato. Saggio su datificazione e diritto*, CLEUP, 2022

C. Sarra (2022-b), *L'uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello*, in "Journal of Ethics and Legal Technologies", vol. 4, 2022, n. 2

P.N. Schwab (2018), *Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40*, in "IntoTheMinds", 28 May 2018

G. Scorza (2022), *In principio era Internet e lo immaginavamo diverso*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A.P. Seminara (2021), *Cookie e libertà del consenso al trattamento dei dati personali*, in "Persona e Mercato", 2021, n. 4

D.J. Solove (2024), *Murky consent: an approach to the fictions of consent in privacy law*, in "Boston University Law Review", vol. 104, 2024

D.J. Solove (2021), *The Myth of Privacy Paradox*, in "The George Washington Law Review", vol. 89, 2021, n. 1

D.J. Solove, W. Hartzog (2024), *Kafka in the Age of AI and the futility of Privacy as Control*, in "Boston University Law Review", vol. 104, 2024

B. Stiegler (2023), *La colpa di Epimeteo*, vol. 1, Luiss University Press, 2023

C. Stokel-Walker (2022), *Privacy policies are four times as long as they were 25 years ago*, in "NewScientist", 3 February 2022

C.R. Sunstein (2017), *#republic. La democrazia nell'epoca dei social media*, il Mulino, 2017

L.Fr.H. Svendsen (2017), *Filosofia della paura. Come, quando e perché la sicurezza è diventata nemica della libertà*, Castelvecchi, 2017

R.H. Thaler, C.R. Sunstein (2014), *Nudge. La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Feltrinelli, 2014

E. Troisi (2019), *AI e GDPR: l'Automated Decision Making, la protezione dei dati, e il diritto alla 'intelligibilità' dell'algoritmo*, in "European Journal of Privacy Law & Technologies", 2019, n. 1

E. Tuccari (2024), *Neuromarketing: un'asistematica disciplina… oltre il consenso?*, in "Persona e Mercato", 2024, n. 2

Z. Tufekci (2018), *The Latest Data Privacy Debacle*, in "The New York Times", 30 January 2018

U.S. Department of Health, Education & Welfare (1973), *Records Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973

Y. Varoufakis (2023), *Tecnofeudalesimo. Cosa ha ucciso il capitalismo*, La nave di Teseo, 2023

A.E. Waldman (2020), *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, in "Current Opinion in Psychology", vol. 31, 2020

M. Weinberger, D. Bouhnik, M. Zhitomirsky-Geffet (2017), *Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior*, in "Oper Information Science", 2017, n. 1

A.F. Westin (1967), *Privacy and freedom*, Atheneum, 1967

J. Zahle (2017), *Privacy, Informed Consent, and Participant Observation*, in "Perspectives on Science", vol. 25, 2017, n. 4

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0216 • articolo sottoposto a peer review • pubblicato in anteprima il 29 apr. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Rosanna Amato

Bridging borders, streamlining justice, balancing interests. The e-Evidence package journey: from a troubled origin story to an uncertain future

The increase in unlawful activities involving online platforms underscores the crucial role of digital evidence in judicial investigations. However, law enforcement and judicial authorities face significant challenges in accessing it. These challenges are particularly pronounced when digital evidence is stored on foreign infrastructures or held by service providers outside the investigation's jurisdiction, as both existing judicial cooperation mechanisms and informal agreements between authorities and service providers have proven inadequate. The EU's e-Evidence package marks a significant development aimed at addressing these challenges. However, despite its innovative nature, it is not without complications. This article explores the main features of the e-Evidence package, emphasising the components that support its functionality. After detailing the system and clarifying its complex elaboration process, the article assesses the potential of the current legal framework to meet its objectives. It focuses on operational aspects and identifies potential issues that may arise during implementation, which could impact its effectiveness.

e-Evidence – Judicial Cooperation – Cybercrime – European Union

Connettere le frontiere, snellire la giustizia, conciliare gli interessi. L'evoluzione del pacchetto e-Evidence: da un esordio problematico a un orizzonte incerto

L'aumento delle attività illecite condotte attraverso le piattaforme online sottolinea il ruolo cruciale delle prove digitali nelle indagini giudiziarie. Tuttavia, le autorità giudiziarie e di polizia incontrano difficoltà significative nell'accesso a tali prove, soprattutto quando queste sono conservate su infrastrutture estere o detenute da fornitori di servizi al di fuori della giurisdizione in cui viene svolta l'indagine. I meccanismi di cooperazione giudiziaria disponibili, così come gli accordi informali tra autorità e provider, si sono infatti rivelati carenti nel garantire un accesso tempestivo ed efficace alle prove digitali. Il pacchetto di norme dell'Unione europea in materia di *e-evidence* rappresenta un'importante evoluzione volta a colmare tali lacune. Tuttavia, nonostante il suo carattere innovativo, questo solleva numerose questioni di natura operativa e giuridica. Questo articolo esamina le caratteristiche principali del pacchetto *e-evidence*, soffermandosi sugli elementi che ne supportano il funzionamento sul piano operativo. Dopo aver delineato l'architettura del sistema e ricostruito il complesso iter che ha portato alla sua finalizzazione, l'analisi si concentra sul potenziale dell'attuale quadro normativo nel perseguire gli obiettivi prefissati. Particolare attenzione è riservata agli aspetti pratici e alle possibili criticità che potrebbero emergere nella fase di attuazione, con il rischio di comprometterne l'efficacia.

e-Evidence – Cooperazione giudiziaria – Crimine informatico – Unione europea

The Author is a researcher at the Institute of Legal Informatics and Judicial Systems of the National Research Council of Italy (office of Bologna)

Summary: 1. Bridging the digital divide. Moving towards new solutions for EU e-Evidence gathering. – 2. The new EU system of e-evidence gathering: how does it work in a nutshell. – 2.1. Digitalising cross-border dialogue for the purpose of gathering e-evidence. – 2.2. Directive (EU) 2023/1544 to designate establishments or appoint legal representatives for the purpose of gathering e-evidence. – 3. A glimpse into the past: legal and political context surrounding the Directive adoption. – 4. Clashing priorities and founding common grounds: the institutional discourse towards a balance between security and fundamental rights. – 4.1. Institutional deadlocks and breakthroughs: towards a unified approach. – 5. A peek into the future. From blueprint to reality: navigating the operational challenges on the Directive roll-out and implementation. – 5.1. Designated establishments and legal representatives' organisational and technical capacity. – 5.2. Shortcomings in operating and technical support tools. – 5.3. Interplay with other legal instruments. – 6. Conclusions.

1. Bridging the digital divide. Moving towards new solutions for EU e-Evidence gathering

Online platforms such as electronic communication services, social networks and marketplaces, together with their applications, increasingly contain information used in unlawful actions. For this reason, they often play a crucial role in judicial investigations, providing vital leads and evidence. The Europol 2023 SIRIUS Report highlights how data disclosed by service providers have been the sole investigative lead in crucial cases involving rape, human trafficking, fraud, phishing scams, aggravated sexual assault, and even terrorism. Without this data, these investigations would have been unsuccessful[1].

Today, a substantial part of criminal investigations depends on electronic evidence, which requires cross-border access to texts, images, emails or messages via apps. Between 2013 and 2016, requests for data from major tech companies such as Google, Twitter, Facebook, Microsoft, and Apple surged by 70%, as reported by EU Commission statistics, with over half of criminal investigations within the EU involving cross-border requests for electronic data. The Commission asserts that in 85% of these investigations, cross-border access to electronic evidence is necessary, with 65% of requests directed towards providers in different jurisdictions[2].

Law enforcement and judicial authorities notoriously struggle with access to such evidence. They often find themselves entangled in cumbersome legal procedures that hinder the swift acquisition of electronic evidence, as most available applicable legal instruments were created before the era of cloud computing and the widespread use of online services. This difficulty is compounded when evidence resides on private infrastructure located abroad or owned by service providers established outside the country where the investigation oc-

1. Europol 2024, pp. 19-20.
2. Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings SWD(2018) 118, 17 April 2018. See also: Casino–Pina–López-Aguilar et al. 2022.

curs[3]. They can rely on various methods to obtain specific data from targeted individuals in criminal investigations, depending on the applicable law and other intervening factors, such as the location of data storage and public accessibility. In all such scenarios, however, acquiring usable evidence typically involves convoluted and lengthy processes. Existing mechanisms for cooperation between authorities have indeed proven inadequate, strained by the increasing number of cross-border cases and the rapid pace at which data can be altered or erased. Moreover, these arrangements are burdened by strict adherence to the principle of sovereignty, particularly in situations involving non-EU countries, where establishing a clear link between the crime and the requested data can be a significant obstacle.

Faced with these limitations, authorities have taken a proactive stance. They have formed partnerships with private service providers on a voluntary basis and thus created informal channels of cooperation running in "parallel" to legal assistance and mutual recognition instruments[4]. As of today, the volume of requests submitted to service providers under these parallel forms of cooperation is disproportionately higher than that of requests submitted through judicial cooperation[5]. Yet, the problem is that such a "voluntary approach" is not subject to any regulation, thereby leading to a complex landscape for competent authorities and service providers alike. On the one hand, the authorities are confronted with a maze of different obligations. These include legal requirements stemming from compliance with national laws, as well as those imposed by individual service providers who, in some cases, may not be willing to cooperate voluntarily at all, citing legal constraints, resource limitations or the lack of relevant policies. Further complicating matters is the admissibility of such data in court, which remains shrouded in uncertainty[6]. On the other hand, these ephemeral forms of collaboration also present a proving ground for service providers. Unclear requests by authorities, different (sometimes even conflicting) obligations, and a varied and ever-changing landscape of sanctions and procedural rules are significant challenges to their internal structure. These providers struggle to keep pace with the ever-evolving policies and regulations, hindering their ability to respond effectively and, in some cases, even deterring cooperation altogether.

In this context, facilitating the swift and legally sound gathering of electronic evidence for criminal investigations and prosecutions across the Union and beyond has become paramount. Notably, the last couple of years marked a turning point in this field, witnessing significant developments in the realm of international cooperation on electronic evidence. A major advancement came with the Second Additional Protocol to the Budapest Convention on Cybercrime, which introduces novel legal bases for direct cooperation to obtain domain name registration information and subscriber data for the purpose of investigations and prosecutions[7]. Moreover, international negotiations on the UN Convention on Cybercrime[8] have made significant progress, focusing on the inclusion of additional chapters which propose the criminalisation of specific cyber-dependent and cyber-enabled activities, providing a framework for international cooperation. Parallel to these developments, negotiations between the EU and the United States have resumed, with the aim to forge an international agreement to remove conflicts of law and facilitate access to electronic evidence[9]. 2023 also marked the enforcement of the EU Digital Services

3. SWD(2018) 118.
4. Sachoulidou 2024.
5. Europol 2024, p. 36 and p. 75.
6. *Ibidem*, p. 41 ss.
7. Council of Europe 2022. See also: Council of Europe 2023.
8. After three years of negotiations, the United Nations Convention against Cybercrime was adopted by the United Nations General Assembly on 24 December 2024 in New York by resolution 79/243. The Convention is the first comprehensive global treaty on this matter, providing States with a range of measures to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes.
9. Wahl 2023, pp 179-180.

Act (DSA) for very large online platforms[10], introducing standardised minimum requirements for orders to provide information under EU Member States' national laws[11].

Beyond these milestones, the most significant development in the field is the adoption of the new EU Electronic Evidence legislative package. This new system represents a legal revolution as it simplifies the process of obtaining electronic evidence in criminal cases by formalising direct requests to private providers of communication, Internet infrastructure service and data storage based in another Member State, generally avoiding the need to involve authorities in the service provider's home country. Although the legislation will not fully enter into force until mid-2026, its approval provides a clear roadmap for EU Member States and service providers to adapt their procedures and ultimately usher in a future of greater legal certainty and efficacy in obtaining electronic evidence across borders.

The EU e-Evidence initiative is composed of two legislative components:

– a Regulation[12] designed to streamline and expedite the process of securing and acquiring electronic evidence that service providers in a different jurisdiction store or possess. It allows national authorities to send an order to preserve (European Preservation Oder) or produce (European Production Order) data directly to the service provider's appointed representative, who is then required to comply by directly delivering the data to the requesting authority.
– a complementing Directive[13] that mandates service providers operating within the EU appoint a legal representative in at least one Member State, thus ensuring that orders and decisions issued under the above Regulation reach the proper recipients.

Designed to work within the existing judicial cooperation framework, these mechanisms do not replace previous instruments but aim to supplement them, particularly the European Investigation Order (EIO). Overall, central to this initiative are (i) simplifying the processes of acquiring and preserving electronic evidence within the EU, (ii) standardising the obligations of service providers, (iii) improving criminal investigations and prosecutions, and (iv) strengthening the protection of individual rights and fundamental freedoms.

Against this backdrop, this article aims to assess the potential of the current legal framework to achieve its objectives. The investigation adopts an operational lens, hypothesising potential challenges that may arise during the implementation phase. To this end, the paper examines the key features of the e-Evidence package, with a particular focus on the core elements underpinning its functionality: the decentralised IT system and the obligations set forth by Directive 2023/1544. Additionally, the article delves into the complex negotiations that culminated in the adoption of the package, with the primary goal of clarifying the motivations and objectives that the European legislator seeks to achieve through this new system. Finally, the analysis explores the Directive's potential benefits alongside its challenges, focusing on organisational and technical capacity, operational and technical tools, and the interplay with other legal frameworks.

This work is, thus, structured into three parts. First, an overview of the new electronic evidence collection system will be provided. This section (paragraph 2) explains the main features and operational mechanisms of the cooperation framework established by the Regulation, including a focus on the decentralised IT system for the exchange of relevant communications and documentation. Then, the Directive's obligations for participating countries, national authorities, and private stakeholders will be detailed. The second section (par-

10. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Art. 10.
11. European Commission 2023.
12. The Regulation lays down the rules and safeguards for national authorities to order service providers located in another Member State to preserve and produce e-evidence for the purpose of carrying out criminal proceedings.
13. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

agraphs 4 and 5) delves into the negotiation and legislative process that led to the finalisation of the e-Evidence package. It highlights the various positions at stake, illustrating how this innovative system navigates the delicate balance between potentially conflicting priorities. This "glimpse into the past" aims to show how the differing views of States, institutional actors, and stakeholders have influenced the achieved outcomes. The final section (paragraph 6), on the other hand, aims to take a "peek into the future" so as to envisage potential challenges and operational issues that might emerge during the implementation phase.

2. The new EU system of e-evidence gathering: how does it work in a nutshell

The new e-Evidence package creates a framework for Member States that outlines how to handle data access requests from authorities within other EU jurisdictions during criminal investigations. Specifically, the Regulation details the type of requests authorities can present to private organisations applicable across the Union when they need to access specific user data for the purpose of obtaining electronic evidence[14] in criminal proceedings: the European Production Order and the European Preservation Order.

The European Production Order is an instrument that allows a judicial authority in one Member State to request and obtain preserved electronic evidence (such as e-mails, texts or app messages, together with information to identify a perpetrator as a first step) within a considerable tight timeframe. On the other hand, the European Preservation Order is a tool that allows a Member State's authority to request that specific data be retained and preserved for a subsequent data production request, thus preventing the deletion or altering of this data. Both are decisions issued or validated by the judicial authority of a requesting Member State.

What makes such a new regime groundbreaking is the mechanism upon which it rests: a direct dialogue between national authorities and private parties, which streamlines the process and aims for higher efficacy. Mirroring other EU judicial cooperation instruments built on the mutual recognition principle, European production and preservation orders utilise standardised multi-lingual templates: the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR)[15]. In addition, they follow standardised procedures, within which pre-defined timeframes and conditions must be met. These critical elements are designed to guide all participants in drafting, transmitting, and executing requests, thereby minimising ambiguities and fostering a level playing field between the requesting and requested parties across Europe.

The authority empowered to issue a European Production Order or Preservation Order hinges on two factors: the specific instrument chosen and the data category requested. This distinction reflects the varying scope of each measure and the differing impact on fundamental rights associated with different types of data.

Notably, when it comes to EPOC-PR, the issuing authority can be a judge, a court, an investigating magistrate or a prosecutor. The same applies to the EPOC, but only if an order must be forwarded to acquire subscriber data and certain traffic data used solely for user identification, such as IP addresses and access codes. A stricter process applies when EPOC involves traffic or content information, which is more intrusive. In these cases, only a judge, court, or investigating magistrate can issue a production order. The Regulation also permits the issuance of EPOC and EPOC-PR by other competent authorities designated by the issuing state, acting as investigating authorities in criminal proceedings and holding the power to gather evidence under national law. However, these orders require validation by a judicial authority to ensure compliance with the Regulation provisions and potentially applicable national law. This prior validation can be waived only in specific emergencies, and even

14. The Regulation defines the term "electronic evidence" as subscriber data, traffic data or content data stored by or on behalf of a service provider in an electronic form (Art. 3(8)), i.e., emails, text messages or content from messaging apps, audio-visual content, or information about a user's online account. These categories are coherent with the EU *acquis*, the EU Court of Justice jurisprudence and other international instruments (e.g., the Convention on Cybercrime of the Council of Europe, Budapest Convention).

15. Regulation (EU) 1543/2023, Art. 9.

then, the issuing authority must obtain ex-post validation within 48 hours.

Once issued, an EPOC or EPOC-PR can be transmitted directly to the service provider operating in one or more Member States, which becomes responsible for executing the request, either by preserving existing data (for EPOC-PR) or producing it (for EPOC). Upon receipt of a European Preservation Order, the service provider is obliged to preserve the requested data for a period of 60 days, after which the preservation duty ceases. However, there are two circumstances that can extend this period: the issuing authority confirms that an EPOC has already been issued or is forthcoming. In these cases, the service provider must retain the data for as long as it takes to produce them.

As far as the EPOC is concerned, it requires a very fast turnaround, as service providers must make the requested data available within 10 days, with an expedited timeframe of 8 hours in emergency situations. Only if the transmitted order targets traffic or content data a suspension period is foreseen[16]. In consideration of the sensitive nature of these types of data, the issuing authority, while forwarding the request to the service provider, has to notify the authority of the requested State (executing authority)[17] and simultaneously forward the standard certificate to it. This will allow the executing authority to assess whether the (few) grounds for refusal provided for in Regulation[18] apply to the case at hand. Such grounds for refusal may be raised within a period of 10 days (or 96 hours in emergency cases). Otherwise, they are deemed not to have been raised, and the strict time limits imposed on service providers remain in effect.

Consultation procedures are foreseen by the Regulation to smooth the dialogue between issuing and enforcing authority. Notably, the issuing authority about to emit an EPOC to obtain traffic or content data may seek prior clarification from the competent authorities of the executing State – directly or through Eurojust or the European Judicial Network – as to whether such data are protected by immunities, privileges granted by the law of the executing State, or other reasons expressly indicated in the Regulation, which may give rise to a legitimate refusal to execute the request[19]. Likewise, before deciding not to recognise or execute an EPOC or EPOC-PR, the executing authority is called upon to consult the issuing authority by any appropriate means for further information, which must be provided within five working days[20].

At the end of this process, should the service provider fail to provide or preserve the evidence requested, a common pecuniary penalty regime applies[21]. The Regulation does not provide for any specifics on this matter but merely stipulates that such financial penalties must be effective, proportionate and dissuasive. However, it requires Member States to ensure that financial penalties of up to 2% of the service provider's total annual worldwide turnover in the preceding business year may be imposed.

2.1. Digitalising cross-border dialogue for the purpose of gathering e-evidence

The Regulation mandates that document transmission and communications for the cooperation mechanism under discussion be conducted exclusively through digital means, with the exception of a few circumscribed situations. This emphasis on digitalisation is notoriously not an isolated effort but rather aligns with a broader strategic and regulatory trend aimed at modernising judicial cooperation by leveraging the potential of available IT tools for the exchange of communications and transmission of documents[22]. Digitalisation is, indeed, increasingly recognised as essential for enhancing the effectiveness and resilience of cross-border judicial cooperation in the EU, which has historically been hampered by reliance on pa-

16. *Ivi*, Art. 10 (2) (4).
17. *Ivi*, Art. 8 (1).
18. *Ivi*, Art. 12.
19. *Ivi*, Art. 5 (10).
20. *Ivi*, Art. 17 (7).
21. *Ivi*, Art. 16 (10).
22. See: "Proposal for a Regulation on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation", Brus-

per-based communication[23]. The rapid expansion of IT applications among individuals, businesses, and institutions – intensified by the urgency of the COVID-19 pandemic – has further accelerated the shift towards fully digital processes, highlighting the necessity of a unified framework where technology is not merely an option but the preferred method for efficient cross-border cooperation[24].

The e-Evidence package embodies this approach by introducing procedures that are, by design, tailored to the digital realm. Barring a few occurrences, it requires all exchanges between competent authorities and private parties to be conducted through a secure and reliable decentralised IT system. This system integrates the IT infrastructures of Member States and Union agencies, utilising interoperable access points for interconnection. Service providers must use this decentralised system via their national IT structures to receive and respond to EPOCs and EPOC-PRs, ensuring swift, direct, and secure cross-border communication while reducing costs and delays for involved parties.

Although the Regulation body does not specify which decentralised system should be used to perform such an exchange, Recital 83 indicates that the access points should be based on e-CODEX (e-Justice Communication via Online Data Exchange)[25]. The e-CODEX system is designed to facilitate cross-border electronic data exchange in civil and criminal judicial cooperation – including text, audio, video, and metadata – thereby enhancing efficacy and access to justice. The system comprises two main components: a gateway for secure message exchange and a connector that links the national gateway to the national application, verifies electronic signatures, ensures message and attachment integrity, supports semantic interoperability, and provides proof of delivery[26].

Such mention in the Regulation's preamble is, after all, not surprising. The e-CODEX system has become crucial to the EU's digital justice strategies. Initiated in 2010 by a consortium of Member States' Ministries of Justice with EU financial backing, the system has continued to evolve and strengthen. Given its pivotal role in cross-border exchanges, it is now established through the EU legal framework, which includes operational and developmental rules, as well as measures to protect fundamental rights in line with the EU Charter of Fundamental Rights. Along with this, the management of e-CODEX will be entrusted to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security, and justice (eu-LISA). This will ensure the system's long-term sustainability and governance while upholding judicial independence. In conjunction with the e-EDES components developed by the EU Commission[27], this system has already shown its practical benefits and is on track to become the main digital solution for secure electronic data transmission in cross-border civil and criminal cases, aiding both in crime fighting and victim involvement. Compared to traditional communication methods, it offers superior standards in terms of speed, secure transmission, data protection, and confidentiality.

2.2. Directive (EU) 2023/1544 to designate establishments or appoint legal representatives for the purpose of gathering e-evidence

The concise description of the system established by Regulation 2023/1543 makes it readily apparent that in order to make the information exchange mechanism between authorities and providers effective, clarity on the players involved and their

sels COM(2021) 759, 1 December 2021; Regulation (EU) 2022/850 of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726; and, two recast regulations from November 2020, that is, the Regulation 2020/1784 of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) and the Service of Documents Regulation.

23. Ontanu 2022.

24. *Ibidem*.

25. Regulation (EU) 2022/850.

26. Velicogna 2014 and Velicogna 2018; Velicogna–Steigenga–Taal–Schmidt 2020.

27. Ben Miloud–Nicolau 2023.

respective responsibilities is imperative. In this context, Directive 2023/1544 is at the heart of the new system of cooperation introduced with the e-Evidence package[28].

The Directive aims to boost legal certainty and effectiveness as it seeks to deter Member States from autonomously addressing legal gaps related to acquiring e-evidence in criminal cases, thus leading to a patchwork of national requirements. Such a scenario has, indeed, not only proved to hinder criminal prosecutions but also to obstruct the seamless provision of services across the internal market. This new piece of legislation's primary aim is to streamline the process of receiving, complying with, and enforcing decisions in a cross-border setting, thereby facilitating the gathering of e-evidence across the EU without overstepping the existing powers of the requested Member State's authorities. Its key element is the obligation for service providers offering services in the Union to designate establishments or appoint legal representatives to handle decisions and orders from Member States' authorities regarding gathering evidence in criminal proceedings. This obligation applies to both EU-established service providers and those outside the EU offering services within it (this is the case for some large companies located in the United States). The sole exemption is for service providers established and operating exclusively within one Member State. Guidelines are laid down concerning where these representatives or establishments should be based, the responsibilities they should hold, and the resources they must rely on to fulfil their obligations, together with a timeline by which service providers must comply with these requirements[29].

As a matter of principle, service providers are free to decide about the number of designated establishments or legal representatives they appoint and in which Member States. Yet, the Directive does not fail to specify that both designated establishment and legal representatives be located in one or more Member States where the service provider operates or is established[30]. Aiming to prevent small and medium-sized enterprises from being disproportionately affected, the Directive allows a single establishment or appointed legal representative to serve several service providers as long as data protection safeguards are maintained[31].

These core provisions are then complemented by ancillary measures that aim to ensure the effectiveness of the stated obligation. On the one hand, Member States are required to appoint central authorities to ensure consistent and proportionate implementation of the Directive[32]. Service providers are then obliged to formally communicate to these central authorities the contact information of their establishment or legal representative, along with any subsequent updates to this information, as stipulated in Article 4. In addition, a sanction regime to deal with possible violations of the obligations under the Directive is established[33].

The overall goal of this framework is to ensure a consistent approach to imposing obligations on both service providers and Member States in the context of electronic evidence collection in criminal proceedings, thereby overcoming challenges arising from divergent national regulations and, most importantly, from dealing with service providers that, while operating in the Union, are located outside it[34].

3. A glimpse into the past: legal and political context surrounding the Directive adoption

The Internet's borderless nature enables the global provision of web services, often bypassing the necessity for physical infrastructure or a corporate

28. Wahl 2023, pp. 165-168.

29. Directive (EU) 2023/1544, Art. 3.

30. According to Directive 2023/1544, Recital 13, the service provider should also designate an establishment in one of the Member States participating in a legal instrument referred to in the Directive.

31. Directive (EU) 2023/1544, Recital 7.

32. *Ivi*, Art 6.

33. *Ivi*, Art 5.

34. The Directive 2023/1544 is effective from 17 August 2023, with a deadline for Member States to incorporate it into national legislation by 18 February 2026.

footprint in the country where the services are accessible. Within the EU internal market, this leads to a diverse landscape of service providers: (i) those operating solely within their home Member State, (ii) those headquartered in one Member State but serving multiple others, and (iii) those located outside the EU yet offering services to one or more Member States, irrespective of their establishment within the EU.

While the Union fundamentally encourages and supports the provision of cross-border services, recognising it as core freedom, this openness poses challenges when services are misused for criminal purposes, turning platforms into critical sources for legally valid evidence in judicial proceedings. Factors such as the inherent volatility and cross-border nature of data, the widespread use of encryption software to safeguard personal information, and the control of such data by private companies create significant challenges for law enforcement and judicial authorities in identifying and collecting data crucial for investigations and criminal proceedings[35]. This is why Member States have consistently identified these challenges as critical issues requiring collective action. Such awareness particularly came to the fore in the aftermath of the terrorist attacks in Brussels, when the tragic events led to the issuance of a joint statement by Justice and Home Affairs (JHA) ministers and representatives of the EU institutions on the urgency of improving the rapid and effective acquisition of electronic evidence by enhancing cooperation with both third countries and national service providers operating on European territory[36]. The same concern was shortly thereafter reiterated in the Council conclusions of 9 June 2016, in which Member States urged the European Commission to prioritise the development of a unified EU strategy to advance criminal justice standards in the digital realm. Harmonised rules at the EU level have been increasingly seen as necessary to foster a more consistent approach to EU criminal law and to remove barriers to the provision of services, thereby improving the functionality of the internal market.

The legal landscape across the Member States has hitherto displayed significant variation in the obligations imposed on service providers, in particular with regard to access to electronic evidence in criminal proceedings, and such fragmentation has inevitably led to legal uncertainty for all stakeholders. Service providers, in particular, typically have to navigate between different and sometimes conflicting obligations and sanctioning regimes, depending on whether services are provided domestically, across borders within the EU or from external jurisdictions. Monitoring nationally applicable policies worldwide and their frequent changes is a demanding task for service providers and require constant adaptation, sometimes including the need to check regional differences within the same country. Just as challenging for the service provider is the handling of the large number of requests, which are only sometimes clear to the recipient, especially if they come from less experienced law enforcement officers. This requires contacting the authority to clarify the contents of the request and the applicable policies and requirements, with a considerable impact, given the large volume of queries they receive. Besides that, even the very authentication of incoming requests is burdensome and entails more than checking verified e-mail domains.

Of course, this burden isn't solely on the shoulders of private actors. National authorities also face a demanding and intricate situation, operating within a murky legal and operational framework. So far, as far as cross-border e-evidence collection is concerned, within the EU, two main channels have been available. The first is relying on the Convention on Mutual Assistance, which, while offering a more advanced form of cooperation compared to typical international patterns, still suffers from significant limitations stemming from the use of traditional routes. A more innovative option is the European Investigation Order (EIO) Directive, introduced in 2017. This instrument follows the mutual recognition model, empowering the issuing judicial authority to directly transmit an investigation order to the competent authority in another Member State for execution. While boasting a

35. Franssen 2024.

36. Extraordinary meeting of Ministers for Justice and Security and representatives of the EU Institutions, Brussels, 24 March 2016.

streamlined procedure and significantly reduced processing times, the EIO is not without its legal and practical challenges. Beyond the many well-known operational issues[37], the system assumes mutual trust and acceptance between the Member States in order to make this streamlined and fast mechanism work. Still, more than twenty years of practical experience in the field show that such trust and acceptance cannot be taken for granted[38]. The truth is that mutual recognition systems, although designed to be "streamlined" and function "out of diversity" perform poorly in the absence of a level playing field and are characterised by an inherent complexity. They heavily depend on the domestic setting, and EIO is no exception. All the more reason why it proves inadequate for obtaining electronic evidence, where time is of the essence.

National legal frameworks in the EU are highly nuanced. A targeted survey of public authorities in the Member States unveiled divergent approaches concerning the connecting factors used to assert jurisdiction over service providers, such as head office, service, or data location[39]. Moreover, these surveys have shed light on service providers' differing responses to requests from foreign law enforcement authorities, resulting in varying reaction times. This discrepancy stems from the diverse regulatory regimes governing whether service providers are obligated to cooperate and the potential sanctions for non-compliance. Further complicating matters are the many regimes implemented at the national level in response to the absence of a general requirement for service providers to establish a physical presence within the Union. These measures exhibit significant variability from one country to another. For instance, there are systems like the German Network Enforcement Act (NetzDG)[40], enacted in 2017, which mandates social network providers to designate a local representative tasked with managing enforcement requests and stipulates fines for non-compliance. In contrast, domestic approaches like the Belgian one do not necessitate local representation but seek to enforce national obligations directly against providers abroad through domestic legal proceedings[41].

Faced with many restrictions, the public authorities have increasingly turned to voluntary collaboration, leading to a fragmented array of informal agreements forged directly with private service providers. As of today, most collaborations between authorities and private parties for the purpose of obtaining electronic evidence are based on voluntary and informal relationships. However, even this situation is far from ideal. These arrangements pose considerable management difficulties and, most importantly, offer unpredictable results[42].

Against this general context, the groundbreaking idea of formalising voluntary cooperation between authorities and private parties at the European level has gained momentum. Central to this system is the requirement for all service providers operating in the Union to designate a specific establishment or legal representative within each Member State where they do business. This designation serves a two-fold purpose. Firstly, it ensures clear identification and proper targeting of evidence-gathering orders in criminal proceedings. Secondly, it simplifies compliance for service providers by establishing a designated contact person responsible for receiving, complying with, and executing such orders on their behalf.

While civil society organisations expressed reservations about the desirability of EU-wide legis-

37. European Judicial Network 2018. On this topic, see also: Mosna 2024; Szijártó 2023; Mitsilegas 2020; Mitsilegas 2019; Amato–Velicogna 2020; Biasiotti 2018; Bachmaier 2018; Amato–Cavallini–Carboni 2018; Sicurella 2018; Marguery 2016.

38. Lenaerts 2017.

39. SWD(2018) 118, p. 133-136.

40. Bundesministerium der Justiz, *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Netzwerkdurchsetzungsgesetz – NetzDG)/*Act to Improve Enforcement of the Law in Social Networks* (Network Enforcement Act), 2017.

41. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226, 17 April 2018.

42. 5th Annual SIRIUS Report, pp 72-73.

lation in this domain, preferring instead to focus EU action on enhancing mutual legal assistance procedures, stakeholders – including service providers – emphasised the importance of ensuring legal certainty in direct collaboration with public authorities and avoiding conflicts of law. This approach, on the other hand, was also advocated by public authorities during the consultation stage. Key concerns they raised during consultations included the challenges of unreliable cooperation with service providers, a lack of transparency, and legal ambiguity surrounding jurisdictional matters related to investigative measures.

Despite converging visions, the legal and political landscape surrounding this initiative was uniquely complex because of multiple factors. Notably, the Directive, which serves as a vital element of the operation of the e-Evidence package, not only intersects different layers of legislation – including national, European and international – but also touches on a broad spectrum of legal domains, ranging from judicial cooperation in criminal matters to data protection and privacy legislation. Also, its evolution has been significantly affected by the need to take into account the law of third countries, especially US law, as major service providers holding crucial evidence fall under its jurisdiction. This nuanced set-up has brought to light the formidable challenges of aligning legal frameworks and ensuring coherent interactions between different jurisdictions' regulatory systems.

4. Clashing priorities and founding common grounds: the institutional discourse towards a balance between security and fundamental rights

The Directive – together with the Regulation – is the result of intense and challenging negotiations. It impacts the field of judicial cooperation with an unprecedented approach that, more than any other instrument in the field, puts the principle of mutual trust to the test. This legislative package offers new possibilities for authorities to pursue criminal investigations that require acquiring electronic evidence across borders. It streamlines processes, thereby navigating challenges inherent in interactions with foreign jurisdictions – challenges that cooperation mechanisms currently in place[43] often find insurmountable. These include the common occurrence of service providers denying access to requested data – either because the requesting authority lacks jurisdiction over the service provider's headquarters location or due to the nationality of the individual whose data is sought – and the unavoidable delays brought on by applying judicial cooperation procedures. Both conventional methods and those founded on the principle of mutual recognition necessitate the participation of the authorities from the State being asked for cooperation, resulting in timeframes that are starkly at odds with the ephemeral nature of electronic data.

The new e-Evidence package was designed precisely to move beyond the constraints of currently available legal instruments and to enhance clarity and legal certainty while significantly expediting the process of obtaining electronic evidence. It imposes an obligation on service providers to respond within 10 days (and, in an emergency, within 8 hours)[44], which is a very tight timeframe compared to the 120-day deadline stipulated in the EIO Directive and, above all, to the average 10 months in traditional mutual legal assistance procedures. This oversimplification, however, makes it all the more difficult to strike an inherently fragile balance between the need to facilitate law enforcement and prosecution in a digital environment on the one hand and the protection of privacy and the other rights of suspects and accused persons on

43. Within the EU legal framework, the cross-border collection of electronic evidence is governed by several legal instruments, including Directive 2014/41/EU on the European Investigation Order in criminal matters, the Council Framework Decision of 13 June 2002 on Joint Investigation Teams, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Regulation (EU) 2018/1727 on the European Union Agency for Cooperation in Criminal Justice (Eurojust), Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol). The matter is also governed by the Mutual Legal Assistance Agreement between the European Union and the United States of America.

44. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Art. 10 (3) and (4).

the other hand[45]. This issue becomes evident when examining the intricacies and debates that characterised the process of establishing the new rules[46].

When the European Commission published its legislative proposal after an extensive two-year preparation process, the new system was met with a mix of support and concerns. On the one hand, key European entities recognised the need for faster access to evidence while strongly emphasising the importance of safeguarding rights. The European Economic and Social Committee (EESC), for instance, highlighted the need for legal representatives within the Union[47], while data protection bodies like the European Data Protection Board (EDPB)[48] and the European Data Protection Supervisor (EDPS) insisted on aligning the new rules with existing data protection laws. They also called for robust safeguards, including judicial oversight and adherence to the Court of Justice of the European Union's (CJEU) case law, to ensure individuals' rights are protected in the process[49]. This strong commitment to fundamental rights was strongly embraced by the European Parliament, which, throughout the legislative process, maintained a highly critical stance on this instrument. On the other hand, the European Council[50] emphasised the critical need for rapid cross-border access to electronic evidence to effectively fight terrorism and organised crime, particularly in light of the US Cloud Act[51], which accentuated the necessity for a cohesive EU strategy to negotiate a binding agreement with the other side of the Atlantic. The same orientation was ultimately adopted by the Council of Ministers, though through a convoluted process[52].

Interinstitutional negotiations started in early 2021 under the Portuguese Council presidency, marked by profound differences between the text of the Council's general approach and the EP's position. After many moments of stalemate, which at times seemed insurmountable, discussions intensified under the French and Czech presidencies. On 29 November 2022, after eight trilogues, the co-legislators reached a political agreement on the most controversial elements of the two proposals. On 25 January 2023, the Council confirmed the agreement with the Parliament and at the end of the same month, the committee approved the agreed text, which was adopted in plenary on 13 June 2023. The final text of both legal tools is not so far from the Commission's original proposals in substance, reflecting a shared belief that more effective legislation is needed to handle cross-border electronic evidence. Nevertheless, the journey towards the adoption of the e-Evidence package was long and marked by intense debate, with deeply

45. Sippel 2023, p. 109; Forlani 2023; Tosza 2023; Christakis 2019.

46. COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency.

47. European Economic and Social Committee, Opinion on the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters [COM(2018) 225 – 2018/0108(COD)] and on the Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [COM(2018) 226 – 2018/0107(COD)], 12 July 2018.

48. European Data Protection Board, Opinion of the EDPB on Commission proposals of the EP and of the Council on European production and preservation orders for electronic evidence in criminal matters, Brussels, 18 October 2018 (OR. en), 13317/18.

49. European Data Protection Supervisor, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, Opinion 7/2019, 6 November 2019.

50. Justice and Home Affairs Council, 11-12 October 2018.

51. The U.S. government adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018 to speed up access to electronic information held by U.S.-based global providers that are critical to foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime.

52. Council of the European Union, Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – general approach, Brussels, 12 December 2018 (OR. en), 15292/18. Ultimately, the Council agreed on its position on the Directive on March 8, 2019. See: Justice and Home Affairs Council, 7-8 March 2019.

divided opinions and significant deadlocks that, at times, suggested that the proposals might be abandoned.

4.1. Institutional deadlocks and breakthroughs: towards a unified approach

After the European Commission introduced its legislative proposal in April 2018, the Council moved relatively quickly to agree on its general approach, adopting positions on the draft Regulation in December 2018 and on the draft Directive in March 2019. Yet, these milestones belied the contentious negotiations underlying the process. Within the Council of Ministers, Member States were divided from the outset[53]. While some supported the Commission's proposals, even advocating for stricter measures – such as real-time monitoring of communication data from emails and messaging platforms for criminal investigations – others were more critical[54]. The dissenting Member States highlighted a lack of sufficient checks and balances in the proposals and expressed concern about the inadequate protection of fundamental rights, underlining the difficulties in crafting legislation acceptable to all parties.

Although the Council reached a general consensus on the legislative approach, the divisions within its ranks were far from resolved. This was evident when eight Member States formally declared their non-support for the compromise proposals[55]. The reservations held extended beyond a general apprehension about the uneven application of the rule of law across the EU[56]. They specifically argued that the compromise proposal fell short of addressing their concerns about the effectiveness of the proposed notification systems. They questioned the ability of the executing State to refuse recognition of an order if there are well-founded reasons to do so. Particularly, there was a call for more robust safeguards, especially concerning orders related to highly sensitive data[57]. These concerns persisted even after interinstitutional negotiations began in January 2021. While a joint position aligned with the Council's general approach eventually emerged, this only occurred after intense debate, due in part to the European Parliament's staunch resistance to certain compromises.

As far as the proposal for a Directive is concerned, national JHA ministers within the Council retained the Commission's criteria regarding the location of legal representatives while incorporating further details on various aspects. These include the extent of their responsibilities, the resources and authority they must possess, the specific duties they are accountable for, and the penalties for non-compliance. Moreover, a significant emphasis was placed on ensuring that these legal representatives could be promptly identified and contacted by the requesting authority[58].

The European Parliament's position, which crystallised in December 2020, added further complexity to the legislative process. Building on preparatory work by the LIBE Committee, the Parliament introduced 841 amendments to the draft Regulation, proposing sweeping changes to its core provisions[59].

At the heart of these amendments was a stronger emphasis on the notification mechanism. Debates centred on whether the Member State hosting the

53. COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency.

54. Justice and Home Affairs Council, 4-5 June 2018, Luxembourg. Ministers from Belgium, Portugal, Cyprus, France, Greece, Italy, and Estonia spoke out to insert a measure into the bill to allow authorities to intercept communication in real-time.

55. Justice and Home Affairs Council (Justice) at the European Council in Brussels, Belgium, 7 December 2018. Germany, the Netherlands, Hungary, Sweden, Finland, Greece, Latvia, and the Czech Republic all voted against.

56. In particular, German Justice Minister Katarina Barley expressed concern that the rule of law is not respected equally throughout the European Union. Cft. Stolton 2018.

57. Letter to Ms Věra Jourová European Commissioner for Justice, Consumers and Gender Equality from the Ministers of the Netherlands, Germany, Czech Republic, Finland, Latvia, Sweden, Hungary, Hellenic Republic.

58. Justice and Home Affairs Council, 7-8 March 2019.

59. European Parliament, Report – A9-0256/2020 of 11 December 2020: Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

service provider or legal representative should play a role in reviewing orders, the specific categories of data subject to such scrutiny, and the scope of the authority's capacity to refuse requests. The Parliament also proposed additional prerequisites for issuing orders, along with a comprehensive list of refusal grounds, some of which would be mandatory[60].

In addition, the Parliament questioned the necessity of the Directive, suggesting that elements of it be incorporated into the Regulation to streamline the legislative framework. This suggestion arose from concerns over the Regulation's legal foundation and the perceived redundancy of the Directive, which required all EU Member States to designate a legal representative, regardless of their participation in the legal frameworks outlined in Title V, Chapter 4, of the Treaty on the Functioning of the European Union (TFEU). The Commission's proposal to potentially expand the role of these legal representatives in future instruments was seen as exceeding its intended scope, raising doubts about its compatibility with Articles 53 and 62 TFEU. Consequently, the Parliament argued that only Member States participating in the Regulation should be required to appoint legal representatives. In response to these critiques, key aspects of the Directive were incorporated directly into the Regulation as a complementary measure under Article 82 TFEU, reflecting the Parliament's strategic efforts to align the legislative framework with its broader vision and legal interpretations.

Interinstitutional negotiations required concessions on both sides. In the second half of 2021, the Council introduced changes to its general approach, thus demonstrating a willingness to compromise beyond its initial position. The adjustments initially brought in (supported by the Member States only as a measure of last resort to overcome the negotiating impasse) did not remove the concerns of the Parliament regarding fundamental rights; therefore, in an attempt to overcome the stalemate, a number of new compromise proposals on the most contentious issues were subsequently tabled. At the same time, previously unresolved issues were revisited. In particular, the resumption of discussions on the draft Directive was promoted, with a view to emphasising the need for its provisions to be kept separate. The conversation was fruitful and resulted in an outcome that gained the approval of the European Parliament. After eight trialogues, and despite the lingering profound disagreement on many crucial issues, the intense negotiating efforts of both the European Parliament and the Council made it possible to reach a political agreement on a final compromise version drafted in late 2022 that gained the support of the Member States delegations and the European Parliament in 2023.

5. A peek into the future. From blueprint to reality: navigating the operational challenges on the Directive roll-out and implementation

Experts, academics, and stakeholders welcomed the adoption of the e-Evidence package, among whom there is consensus that it is a milestone in the collaboration between authorities and service providers. Most service providers have also valued the new rules. They see them as bringing much-needed legal certainty to the process of disclosing data in criminal investigations. The new system will eliminate or significantly reduce the current burden they face in assessing the legitimacy of each request as, previously, service providers had to navigate a complex legal landscape with many applicable national laws and international instruments. Furthermore, the standardisation of the format for data disclosure and retention orders has been widely praised for its positive impact on managing these requests at an operational level[61]. Nevertheless, many voices have been and still are critical of the overall new system of access to e-evidence. Beyond the delicate balance of competing interests[62], doubts indeed arise as to the system's practical viability, in respect of which the successful implementation of the Directive and the smooth functioning of the decentralised IT system are prerequisites.

Notably, three primary challenges are supposed to hinder the successful implementation of this system: (a) the organisational and techni-

60. Christakis 2023.

61. 5th Annual SIRIUS Report, p 75.

62. Berthélémy 2023; Tosza 2021; Tosza 2024; Mitsilegas 2018.

cal capacity of the service providers, specifically their appointed offices and legal representatives, required to intervene in the procedure envisaged by the e-evidence package; (b) underlying issues related to the effective functioning of certain operational and technical tools designed to support the procedures; and (c) the complex interplay of legal frameworks of collaboration that affect the overall effectiveness of the system.

5.1. Designated establishments and legal representatives' organisational and technical capacity

Several factors can influence the organisational and technical capacity of designated establishments and legal representatives (see Tab. 1). Key among these are ambiguities in the relevant regulations together with financial and non-economic burdens associated with managing procedures. Problems with substantial operational repercussions are likely to be caused by the unclear rules establishing the criteria for determining the designated establishment or legal representative. The Directive mandates that service providers, including those outside the EU, establish them within the Member States territory so as to ensure accessibility for requests by foreign authorities regarding the production or preservation of e-evidence. Guidance on how to identify these establishments or representatives, however, is so far missing, thus allowing discretion and leading to uncertainty for companies. According to the Directive, a "substantial connection" to the Member States where services are offered is pivotal for determining the service provider's obligations. Yet, defining what a "substantial connection" actually is remains ambiguous, especially in cases where the service provider does not have a physical establishment in the Member State. The criteria hinge on having a significant user base or targeting activities towards one or more Member States, both vaguely defined. In the Impact Assessment, the option to specify a "significant user base" was considered but ultimately discarded due to challenges in setting and applying a specific threshold and the risk of creating exploitable loopholes, suggesting a preference for inclusiveness. Similarly, the determination of "targeting of activities" is subject to unclear factors[63]. Consequently, service providers face uncertainties in determining their obligations under the Directive and understanding sanctions, potentially leading to inconsistent compliance and enforcement of the Directive's requirements.

Alongside this, operational challenges are likely to arise due to the financial and non-financial burdens that fulfilling the obligations of the new e-evidence collection system will entail, particularly for non-EU SMEs. While direct cooperation with private entities is designed to cut costs and boost efficiency, the transition to this new collaborative framework will impose a higher financial burden on these private actors. Consider, for instance, the costs associated with designating entities under Directive 1544/2023/EU within the EU. Even though "the designated establishment or legal representative may be shared among several service providers, particularly SMEs"[64], this approach could still impose a significant burden on the business community. Service providers must cover all expenses related to the establishment, maintenance, and management of their legal representative or designated establishment to ensure compliance with the Directive. This includes costs for data transmission or backup, with the possibility of reimbursement dependent on the laws of the issuing state allowing such reimbursements for similar national orders[65].

Both financial and non-financial burden is also expected to adjust private entities' structures to comply with requests from other Member States' authorities, in accordance with the stipulated regulations[66]. Immediate and comprehensive responses to authority requests require stringent technical procedures and a skilled team ready to meet tight deadlines[67], all the more so that poten-

63. Regulation (EU) 2023/1543, Art. 3 (4) lett b; Recital 30.

64. Directive (EU) 1544/2023, Recital 7.

65. Regulation (EU) 2023/1543, Art. 14; Recital 68.

66. SWD(2018) 118. See also: Cuadrado Salinas 2023.

67. Juszczak–Sason 2023, pp. 182-200; Schauenburg–Zapf–Rossbrey–Málaga 2023.

Category	Key Issues	Operational Implications
Regulatory Ambiguities	- *Unclear designation criteria*: Ambiguous rules on how to identify a legal representative or designated establishment. • "Substantial connection" dilemma; • Vague "user base"/"targeting" criteria.	- *Uncertain obligations and sanctions*: Providers struggle to understand their exact responsibilities and risk inconsistent enforcement. - *Discretion in application*: Divergent interpretations can lead to uneven compliance and potential legal disputes. - *Higher legal risk*: Inability to pinpoint when penalties might apply or which criteria trigger full Directive obligations.
Financial/Non-Financial Burdens	- *Establishment and maintenance costs*: Setting up and running a designated establishment or legal representative entails fees for infrastructure, staffing, and administration. - *Potential reimbursement gaps*: Whether costs (e.g., data transmission, backup) are recoverable depends on national laws. - *Particular strain on SMEs*: Shared representatives are allowed but may still impose considerable overhead. - *Non-economic burdens*: Internal reorganisations, compliance procedures, and increased documentation demands add to the overall load.	- *Heightened financial strain*: Smaller companies or non-EU entities risk higher cost impacts, including fines for non-compliance. - *Vulnerability to penalties*: Even minor infractions can trigger sanctions that can weigh heavily on SMEs.
Technical Capacity	- *Stringent demands and Directive's silence on technical standards*: Specific expertise is needed to identify problematic aspects, challenge unjustified requests and navigate diverse legal frameworks for electronic evidence.	- *Complex compliance architecture*: Heightened administrative burdens and coordination challenges arising from the need of continuous adaptation to multiple legal frameworks and potential confusion about standards of proportionality and necessity.
Skills	- *Multidisciplinary expertise*: Beyond legal know-how, technical and linguistic proficiency is needed to review requests accurately, including verifying certificates and documentation. - *Limited support networks for private actors*: Companies lack the resources available to national authorities (e.g., established liaison channels and networks).	- *Higher demand for specialized staff*: Legal representatives or designated establishments must detect problematic requests and raise challenges where necessary. - *Steep learning curve for SMEs*: Smaller businesses can face disproportionate difficulty acquiring the mix of legal, technical, and language skills. - *Potential for procedural bottlenecks*: Inadequate expertise can delay or derail the timely exchange of information, increasing the risk of fines or legal disputes.

Tab. 1 — *Organisational and Technical Capacity Challenges from an Operational Perspective*

tial violations can result in financial penalties[68]. These penalties, while perhaps a minor deterrent for large companies like Google, could impose a disproportionate financial strain on smaller com-

68. Cuadrado Salinas 2023.

panies[69]. Additionally, designated establishments or legal representatives who are jointly and severally liable with service providers cannot invoke unauthorised data transmission or inadequate internal procedures as a defence against non-compliance.

While the Directive fails to detail technical capacity requirements, legal representatives or designated establishments must possess specific expertise to identify any problematic aspects of requests and challenge, where appropriate, any foreign authority request that may seem unjustified or potentially infringe on privacy due to governmental overreach[70]. Navigating this complex landscape is challenging, especially with different prerequisites for issuing orders[71] and the absence of explicit justifications for proportionality and necessity in some cases[72]. The "variable geometry" of prerequisites for issuance and guarantees of proportionality and necessity introduces diverse coordination patterns and potential administrative burdens arising from managing different national frameworks for obtaining electronic evidence[73].

Yet there is a further level of complexity to consider, especially when it comes to the technical skills of those who perform these procedures. The expertise required to conduct such operations is not merely legal. While tasks such as discerning the legitimacy of a certificate or identifying problems in received documentation are generally acknowledged as challenging, particularly in a multilingual context, it is often overlooked that in managing cross-border cooperative procedures, seemingly trivial practical issues can be even more insidious. Decades of experience with mutual recognition cooperation models have revealed numerous difficulties inherent in these processes, which are likely to be even more severe for private entities lacking the substantial expertise, resources, and support networks available to judicial and police authorities since the adoption of the European Arrest Warrant.

5.2. Shortcomings in operating and technical support tools

The e-Evidence package introduces essential operational support tools to make carrying out application and compliance procedures feasible. However, inherent systemic issues make using these tools challenging (see Tab. 2).

A particularly relevant example in this context is Article 4(4) of the Directive, which mandates the creation of a repository on the European Judicial Network's webpage. Member States are required to compile information about the establishments and legal representatives designated by service providers, including contact details, accepted receiving languages, and the precise territorial scope when a service provider designates multiple establishments or appoints multiple legal representatives. This measure is welcome, as the creation and maintenance of a dedicated repository is essential to enable competent authorities to identify the correct recipient, thereby ensuring the functionality of the system, especially when a service provider has multiple establishments or representatives. Yet, this represents a typical illustration of a seemingly simple but practically demanding operational challenge. The establishment of effective national notification systems between service providers and central authorities cannot be taken for granted. Recent research project findings reveal the complexities involved in what may seem like

69. Article 5 of the Directive mandates that Member States set up a system of "effective, proportionate, and dissuasive penalties", which, according to Regulation Article 15, could include fines of up to 2% of a service provider's total annual worldwide turnover from the previous year. Still, the absence of detailed guidelines on what constitutes "effective, proportionate, and dissuasive penalties" may result in inconsistent application across the EU. This inconsistency could lead to legal uncertainties for businesses operating in multiple Member States, fostering varied compliance challenges and escalating operational costs. Moreover, this ambiguity could weaken the Directive's effectiveness, as insufficient deterrent penalties might fail to encourage compliance, complicating enforcement efforts further.

70. Art. 11 (4) Regulation EPOC. See Sarkowicz 2022, pp. 101-110.

71. Regulation 1543/2023/EU, Art. 5 (2) and Art. 6 (2).

72. Busillo 2023.

73. *Ibidem*.

Category	Key Shortcomings	Operational Impact
Systematising Contact Details (Repository)	- *Complexity of Article 4(4) repository*: Although seemingly straightforward, setting up and maintaining accurate contact details databases of service providers can be demanding and challenging in practice.	- *Potential for misdirected or delayed requests*: If repository data are incomplete or outdated, authorities can struggle to identify the correct recipient. - *Increased administrative overhead*: Providers and authorities must devote time and resources to keep listings accurate and current. - *Risk of partial or ineffective solutions*: Without fully addressing underlying complexities, any repository-based tool might fail to function as intended across different Member States.
Decentralised IT System Functioning	- *Limited e-CODEX deployment:* Many Member States lack an operational access point for new procedures. - *Volume constraints*: e-CODEX sets size limits on data transmission, requiring alternative channels for large data sets. - *Rapidly evolving requirements*: Technological advances and shifting legal frameworks can outpace the integration process if not proactively managed.	- *Delayed or incomplete data exchanges*: Without fully configured access points or alternative channels, transmitting electronic evidence promptly can be difficult. - *Challenges for private actors (SMEs in particular)*: Adapting to e-CODEX and related systems demands specialised IT capacity and resources. - *Escalating costs and compliance risks*: Entities that postpone updating or expanding their technical infrastructure may face higher expenses and potential penalties by the end of the implementation period.

Tab. 2 — *Shortcomings in Operating and Technical Support Tools*

the straightforward technical task of creating databases for the electronic addresses of authorities responsible for executing orders (e.g., EIO)[74]. These insights highlight that such informative tools are not merely technical solutions but involve IT, legal, and organisational dimensions influenced by various non-technical and contextual factors. A comprehensive understanding of these elements is vital to develop the system effectively for its intended use and ensure its relevance in a rapidly evolving technological and societal landscape.

Along with this, it's crucial to acknowledge the potential difficulties in aligning the IT systems of designated establishments and legal representatives with the decentralised IT system used for secure communications and exchanges, likely to be e-CODEX. Designed as a content-neutral e-delivery platform, e-CODEX integrates with existing national and European e-Justice IT systems rather than replacing them[75]. While this theoretically simplifies access and use, practical challenges remain, especially as the e-evidence system expands access to private entities. To begin with, each e-CODEX participant requires an access point to join the network. This access point can either be the one provided by the Commission or an alternative at the national level. However, many Member States currently lack an access point and still necessitate gateway connector installation by trusted authorities. Even when a national access

74. See, for instance, the results of the CCDB Project, which was launched to establish an EU Criminal Court Database (CCDB) by collecting contact data on all judicial bodies of the Member States and project partners States responsible for proceedings related to issuance of EIOs.

75. Regulation (EU) 2022/850 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system). See: Ontanu 2023; Velicogna–Steigenga–Taal–Schmidt 2020; Velicogna 2018.

point is available, it must be configured for specific cooperative procedures, currently available only for the EIO[76]. Furthermore, two additional considerations must be addressed. The first concerns the contact list that the authority must use to forward communications and requests to private parties. It is not sufficient for this list to be merely available on the European Judicial Network's dedicated page. For the authority to be able to use this directory to send requests or communications, it needs to be integrated with the e-Codex system. Secondly, while the e-CODEX system is primarily designed for the exchange of communications, data exchange is possible only if it does not exceed a certain volume. Therefore, a different channel will be necessary for transmitting larger volumes of data. In conclusion, proactively addressing technical and usability issues is crucial to avoid potential costs and non-compliance problems at the end of the three-year implementation period.

5.3. Interplay with other legal instruments

While not the main focus of this article, it's important to recognise that the complex international legal landscape could have operational implications (see Tab. 3). Notably, the e-Evidence package fits into a broader array of national, regional, and international mechanisms that integrate the private sector into government crime-fighting initiatives[77]. As such, the e-Evidence package is designed to complement existing legal frameworks, leading to various patterns of cooperation[78], though the specifics of its interaction with these frameworks are yet to be defined.

In this respect, the interaction between the EIO Directive with Directive 1544/2023 warrants particular attention. Judicial authorities in the Member States retain discretion in selecting the most suitable instrument for each case, potentially preferring the EIO for its extensive scope in requiring the production of digital evidence, among other investigative measures. However, it must be noted that the EIO Directive offers limited details on accessing electronic evidence. Furthermore, requests for evidence via the EIO cannot bypass inter-authority collaboration, as they must adhere to the mutual recognition instruments' standard procedure. For service providers, the enforcement request for the EIO originates from the executing authority in the host country of the legal representative or designated establishment following a prior evaluation. This multi-tiered process may pose challenges for executing requests, especially given the varying cooperation modes and responsibilities imposed on the provider.

A further critical limitation of the Directive is its actual inability to address challenges stemming from the domestic laws of non-EU service providers. Notably, "blocking statutes" such as those within the U.S. Electronic Communications Privacy Act, which restrict U.S. service providers from sharing content data with foreign authorities, significantly hinder cooperation with EU law enforcement[79]. The European Commission acknowledges this hurdle, emphasising its persistence until a bilateral U.S.-EU agreement is established. This situation underscores the intricate interplay between international law and national legal frameworks governing cross-border data access and transfer[80]. A pivotal development in this sphere is the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018. This legislation empowers the U.S. to negotiate "executive agreements" with foreign countries, facilitating reciprocal access to data held by each nation's service providers. Such agreements would authorise U.S. service providers

76. The EU has employed Reference Implementation Software in criminal proceedings, notably for the European Investigation Order (EIO) as part of the e-EDES Infrastructure, which operates on the e-CODEX platform. In the civil sphere, comparable tools are under development to support the revised regulations for the Service of Documents and the Taking of Evidence. These initiatives include the creation of the Reference Implementation Software for the Service of Documents (SoD) and for Taking of Evidence (ToE). See Ontanu 2023, p. 96 ss.

77. Brière 2021; González Fuster–Vázquez Maymir 2020; Signorato 2023; Mitsilegas 2014.

78. Directive 1544/2023/EU, Art. 1.

79. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Explanatory Memorandum, Strasbourg, 17 April 2018, COM(2018) 225, 2018/0108(COD), p. 11.

80. Franssen 2018.

Category	Key Points	Operational Implications
Interaction with EU Instruments	- *Broader legal ecosystem*: The e-Evidence package complements existing EU frameworks, though exact cooperative patterns remain to be clarified.	- *Choice of instrument uncertainty*: Service providers must respond differently depending on whether authorities use the EIO or e-Evidence procedures, creating administrative complexity. - *Parallel obligations*: Overlapping requirements can cause confusion regarding enforcement and responsibilities.
Interaction with Non-EU Instruments	- *Blocking statutes*: Certain non-EU laws prohibit service providers from sharing content data with foreign authorities, limiting compliance with EU demands.	- *Legal conflicts for providers and continued uncertainty*: Non-EU companies may be unable to comply with EU orders if barred by home-country laws, risking enforcement deadlock and potential liability on both sides. Service providers can face ambiguous obligations when data are stored under differing legal regimes.

Tab. 3 — *Interplay with Other Legal Instruments*

to comply with valid legal requests from partner countries for content data. Negotiations for a similar EU-U.S. agreement commenced in 2019 but were temporarily suspended to align with European electronic evidence legislation. Resuming in 2023, these talks remain complex and uncertain as both parties grapple with the prospect of potentially relinquishing sovereign data access rights, irrespective of data location[81].

6. Conclusions

A substantial part of criminal investigations in the EU today necessitates access to information found on online platforms like communication services, social networks, and marketplaces. However, authorities face significant challenges in obtaining such cyber evidence due to its transient nature and the frequent need for cross-border cooperation, as the data are often stored abroad or managed by foreign service providers. Essentially, when dealing with electronic evidence, cross-border cooperation reaches the highest levels of complexity, as beyond the usual difficulties inherent in such collaborations, the nature of electronic evidence introduces further complications. Its volatility and susceptibility to alteration or deletion make the timing of evidence collection even more crucial.

Although a major effort has been made to streamline cross-border judicial cooperation over the past two decades, law enforcement and judicial authorities still encounter significant challenges in accessing electronic evidence. Even state-of-the-art instruments based on the principle of mutual recognition have struggled to keep up with the challenges posed by new digital evidence. Not surprisingly, the direct authority-to-authority dialogue, mandated to conclude within the three-month timeframe established by the EIO, has proven ineffective in a field where time is of the essence.

In addressing these challenges, authorities have increasingly turned to informal partnerships with private service providers. However, this unregulated approach, while seemingly more effective on paper, presents complications for both the requesting and requested parties. Cooperation for obtaining electronic evidence occurs within a cumbersome and diverse legal landscape, as domestic systems differ significantly in key areas (e.g., jurisdictional linkage factors, obligations to provide necessary information, sanction structures, and mandates for companies to establish local offices). This diversity leads to inconsistent obligations for recipients, which affects response times to evidence-collection

81. Bachmaier 2023; Propp 2023.

requests and the willingness to cooperate. Moreover, it creates uncertainties about the admissibility of any obtained evidence, further complicating the efforts of authorities.

The pressing need to move beyond these limitations has sparked a vigorous debate in the EU, prompting the European Commission to come up with effective legislative solutions aimed at offering greater clarity and certainty in the cross-border evidence-collection process. As a result of two years of work, a highly innovative proposal for a legislative package was brought forward to respond to this sense of urgency. The proposed new system for e-evidence gathering relied on the architecture of the most advanced cooperative tools based on the principle of mutual recognition, standardising processes, conditions, and templates, but it went much further. It envisioned more streamlined procedures and very short response times and, most importantly, established unprecedented legal bases for formalising direct dialogue between judicial authorities and private actors. Although much-awaited, the proposal was met with conflicting reactions, which were very clearly echoed during the negotiation process, which was anything but smooth. The discourse surrounding the e-Evidence package has been heated. The new system's plan for oversimplification sparked criticism and caused a significant rift among institutions concerning the issues that could arise from the fragile balance between the need for rapid investigative activities and the rights of the accused. Despite these clashing perspectives and the many moments of seemingly insurmountable deadlock, the collective agreement on the need for more effective measures in this area prevailed, and a final solution was achieved that remains fairly close to the initial proposal.

Mirroring previous mutual recognition instruments in the field of judicial cooperation, the new system creates a defined cooperative path between requesting and requested parties for the delivery of EPOCs or EPOC-PRs, i.e., standard certificates with which it is possible to request the production of evidence or its preservation, depending on the case. The response time is very short, in urgent cases even just a few hours, and the reasons that recipients can use to refuse compliance are very limited. Moreover, there is a penalty regime in case of non-compliance, which should discourage divergent behaviour.

Particularly noteworthy for this analysis are the requirements outlined in Directive (EU) 2023/1544 and the provisions within the Regulation mandating the use of a decentralised IT system for exchanging communications and documentation between parties involved. Organisation and technology are indeed pivotal factors for the deployment of these procedures. Previous research in the field of EU judicial cooperation, after all, has long indicated that relying solely on legal remedies cannot be sufficient to close the enforcement gaps of mutual recognition instruments, and the new e-Evidence package is by no means an exception.

In this context, the Directive's requirement for service providers to designate establishments or legal representatives within the EU is crucial for ensuring the effective transmission and execution of EPOCs and EPOC-PRs. This requirement becomes particularly significant when dealing with non-EU companies operating in the European market. While the Regulation defines the procedural steps, conditions, and requirements, the Directive makes these procedures practical by identifying the responsible parties. It clarifies who will receive, execute, and be held accountable for requests, thereby enhancing enforcement, oversight, and compliance with the EU Regulation. Though not explicitly aimed at consumer protection, these measures contribute to a more regulated and transparent environment, indirectly supporting consumer interests by ensuring adherence to EU standards. Furthermore, mandating electronic transmission as the designated cross-border communication route, rather than an optional method, is a positive development. Digitising the process with state-of-the-art IT solutions promises operational benefits, including a more streamlined, secure, and reliable exchange of information. The Regulation's requirement for digital communication aligns with broader efforts to modernise and improve cross-border judicial processes. This shift towards digital systems, such as e-CODEX, is expected to enhance efficiency, resilience, and cost-effectiveness by replacing traditional paper-based methods. Managed by eu-LISA, these systems ensure interoperability, protect data, and maintain confidentiality, supporting more sustainable and efficient operations and contributing to the rapid resolution of cross-border civil and criminal cases.

Nevertheless, these key operational components come with their own set of critical challenges, particularly at the system level, where they can compromise overall functionality and effectiveness. Beyond issues arising from the interaction between the e-Evidence package and the existing legal framework, as well as limitations due to conflicts of law, there are two main sets of challenges likely to impact the practical feasibility of the new system. First, there are concerns about the capacity of private actors, especially smaller service providers, to effectively respond to cooperation requests. These challenges stem from unclear regulations, financial and operational burdens, and technical complexities. The complexity of cross-border cooperation procedures can be overwhelming for inadequately equipped private entities, potentially leading to paralysing effects and exposure to penalties. Additionally, there are issues related to the operational and technical support tools created by the legislation to support the system. Although these tools are intended to serve an enabling or supplementing function, they themselves may be difficult to implement. Examples include the creation of the European Judicial Network's repository and its integration into the decentralised IT system architecture, as well as ongoing functionality problems with the e-CODEX system.

In essence, the success of the new cross-border electronic evidence collection system is likely to depend on how effectively various operational aspects are managed. This includes addressing measures that may appear minor or straightforward but are, in reality, pivotal to the system's overall viability. Properly handling these details can be key for ensuring the system's functionality and effectiveness.

References

R. Amato, D. Cavallini, N. Carboni (2018), *Italian National Report*, in T. Marguery (ed.) "Mutual Trust under Pressure, the Transferring of Sentenced Persons in the EU: Transfer of Judgments of Conviction in the European Union and the Respect for Individual's Fundamental Rights", Wolf Publications, 2018

R. Amato, M. Velicogna (2020), *Encoding Cross-Border Judicial Cooperation in Criminal Matters: Current Practices and the Rise of the EU E-Justice Infrastructure*, in C. Billet, A. Turmo (eds.), "Coopération opérationnelle en droit pénal de l'Union européenne", Bruylant, 2018

L. Bachmaier (2023), *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings?*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

L. Bachmaier (2018), *Mutual Recognition and Cross-Border Interception of Communications: The Way Ahead for the European Investigation Order*, in C. Brière, A. Weyembergh (eds.), "The Needed Balances in EU Criminal Law: Past, Present and Future", Hart Publishing, 2018

D. Ben Miloud, C. Nicolau (2023), *e-Evidence Digital Exchange System (eEDES)*, in M.A. Biasiotti, F. Turchi, "European Investigation Order. Where the Law Meets the Technology", Springer, 2023

C. Berthélémy (2023), *e-Evidence compromise blows a hole in fundamental rights safeguards*, in "European Digital Rights (EDRI)", 2023

M.A. Biasiotti (2018), *Present and Future of the Exchange of Electronic Evidence in Europe*, in M.A. Biasiotti, J.P. Mifsud Bonnici, J. Cannataci, F. Turchi (eds.), "Handling and Exchanging Electronic Evidence Across Europe", Springer, 2018

M.A. Biasiotti, F. Turchi (eds.) (2023), *European Investigation Order. Where the Law Meets the Technology*, Springer, 2023

S. Busillo (2023), *Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore*, in "Freedom, Security & Justice: European Legal Studies", 2023, n. 3

C. Brière (2021), *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, in "European Papers", vol. 6, 2021, n. 1

F. Casino, C. Pina, P. López-Aguilar et al. (2022), *SoK: cross-border criminal investigations and digital evidence*, in "Journal of Cybersecurity", vol. 8, 2022, n. 1

T. Christakis (2023), *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive*, in V. Franssen, S. Tosza (eds.), "The Cambridge Handbook of Digital Evidence in Criminal Matters", Cambridge University Press, 2023

T. Christakis (2019), *E-evidence: the way forward* (Summary of the Workshop held in Brussels on 25 September 2019), in "European Law Blog. News and Comments on EU Law", 2019

Council of Europe (2023), *T-CY Guidance Note #13, The scope of procedural powers and of international cooperation provisions of the Budapest Convention*, 27-28 June 2023

Council of Europe (2022), *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224), 2022

C. Cuadrado Salinas (2023), *La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?*, in "Ius et Scientia", vol. 9, 2023, n. 2

European Commission (2023), *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, Brussels, 25 April 2023

European Judicial Network (2018), *51st EJN Plenary meeting – Conclusions on the application of mutual recognition instruments*, Brussels, 5 December 2018 (OR. en), 14754/18

Europol – European Union Agency for Law Enforcement Cooperation (2024), *5th Annual SIRIUS EU Electronic Evidence Situation Report*, The Hague, November 2023 (updated version 11 April 2024)

G. Forlani (2023), *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

V. Franssen (2024), *Cross-border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the e-Evidence Regulation*, in M. Bergström, V. Mitsilegas, T. Quintel (eds.), "Research Handbook on EU Criminal Law", 2nd ed., Edward Elgar, 2024

V. Franssen (2018), *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, in "European Law Blog. News and Comments on EU Law", 2018

G. González Fuster, S. Vázquez Maymir (2020), *Cross-border Access to E-Evidence: Framing the Evidence*, Center for European Policy Studies (CEPS), 2020

A. Juszczak, E. Sason (2023), *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice An Introduction to the New EU Package on E-evidence*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

K. Lenaerts (2017), *La vie après l'avis: exploring the principle of mutual (yet not blind) trust*, in "Common Market Law Review", vol. 54, 2017, n. 3

T. Marguery (2016), *Rebuttal of Mutual Trust and Mutual Recognition in Criminal Matters: Is 'Exceptional' Enough?*, in "European Papers", vol. 1, 2016, n. 3

V. Mitsilegas (2020), *Trust*, in "German Law Journal", Special Issue 1: "20 Challenges in the EU in 2020", vol. 21, 2020

V. Mitsilegas, (2019), *The European Model of Judicial Cooperation in Criminal Matters: Towards Effectiveness based on Earned Trust*, in "Revista Brasileira de Direito Processual Penal", vol. 5, 2019, n. 2

V. Mitsilegas, (2018), *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in "Maastricht Journal of European and Comparative Law", vol. 25, 2018, n. 3

V. Mitsilegas, (2014), *Transatlantic counterterrorism cooperation and European values: The elusive quest for coherence*, in E. Fahey, D. Curtin (eds.), "A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders", Cambridge University Press, 2014

A. Mosna (2024), *Judicial Protection in EU Cross-Border Evidence-Gathering: the EIO as a Case Study*, in "EuCLR European Criminal Law Review", vol. 14, 2024, n. 2

E.A. Ontanu (2023), *The digitalisation of European Union procedures: A new impetus following a time of prolonged crisis*, in "Law, Technology and Humans", vol. 5, 2023, n. 1

E.A. Ontanu (2022), *Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure*, in "Oñati Socio-Legal Series", vol. 12, 2022, n. 3

K. Propp (2024), *Navigating Toward an EU-U.S. Agreement on Electronic Evidence*, in"Lawfare", 1 December 2023

A. Sachoulidou (2024), *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation*, in "New Journal of European Criminal Law", vol. 15, 2024, n. 3

J. Sarkowicz (2022), *Legal representative in the proceedings of gathering e-evidence under European Production Order: de lege lata remarks and de lege ferenda postulates*, in "EuCLR European Criminal Law Review", vol. 12, 2022, n. 1

T. Schauenburg, D. Zapf, N. Rossbrey, F. Málaga (2023), *EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations*, in "White & Case", 2023

R. Sicurella (2018), *Fostering a European criminal law culture: In trust we trust*, in "New Journal of European Criminal Law", vol. 9, 2018, n. 3

S. Signorato (2023), *Cross-Border Gathering of E-Evidence: Different Legal Frameworks in European Union and Council of Europe*, in "Journal of Eastern European Criminal Law", 2023, n. 1

B. Sippel (2023), *Guest Editorial*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

S. Stolton (2018), *Council makes half-hearted agreement on e-Evidence*, in "EURACTIV", 2018

I. Szijártó (2023), *The Interplay Between the European Investigation Order and the Principle of Mutual Recognition*, in "European Papers", vol. 8, 2023, n. 3

S. Tosza (2024), *Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights*, in "Common Market Law Review", vol. 61, 2024, n. 1

S. Tosza (2023), *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?*, in "European Data Protection Law Review", vol. 9, 2023, n. 2

S. Tosza (2021), *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in "Computer law & Security review", vol. 43, 2021

M. Velicogna (2018), *e-Justice in Europe: From National Experiences to EU Cross-Border Service Provision*, in L. Alcaide Muñoz, M.P. Rodríguez Bolívar (eds.) "International e-Government Development. Policy, Implementation and Best Practices"w, Palgrave Macmillan, 2018

M. Velicogna (2014), *Coming to Terms with Complexity Overload in Transborder e-Justice: The e-CODEX Platform,* in F. Contini, G.F. Lanzara (eds.), "The Circulation of Agency in E-Justice", Springer, 2014

M. Velicogna, E. Steigenga, S. Taal, A. Schmidt (2020), *Connecting EU Jurisdictions: Exploring How to Open Justice Across Member States through ICT*, in "Social Science Computer Review", vol. 38, 2020, n. 3

T. Wahl (2023), *E-evidence Regulation and Directive Published*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0220 • articolo sottoposto a peer review • pubblicato in anteprima il 7 mag. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Marco Guerra

Le prospettive di collaborazione tra Autorità indipendenti nell'era digitale

L'articolo analizza la natura e il ruolo delle Autorità amministrative indipendenti nell'odierno contesto digitale, focalizzando l'attenzione sulla necessità di attuare una sinergia sempre più intensa tra tali organismi a tutela dei diritti e delle libertà fondamentali degli individui. A fronte della compenetrazione delle rispettive sfere di competenza e dell'assenza di norme di legge che delineino una disciplina organica dei rapporti tra Autorità, è dovuta intervenire la giurisprudenza, che ha affermato il principio di leale cooperazione tra le stesse. Per di più, le criticità legate a tale situazione sono destinate ad aumentare, viste le iniziative normative assunte dall'Unione europea al fine di promuovere lo sviluppo del settore digitale e di regolamentarlo; per tale ragione, si rende inderogabile un intervento a livello europeo e nazionale del legislatore o delle Autorità stesse volto a razionalizzarne le forme di raccordo ed interazione al fine di offrire adeguate garanzie per i diritti delle persone.

Autorità indipendenti – Leale cooperazione – Costituzionalismo – Governance digitale

Prospects for cooperation among independent Authorities in the digital era

This paper examines the nature and role of independent administrative Authorities within the current digital context, placing particular emphasis on the growing need to foster stronger synergies among such bodies in order to safeguard the fundamental rights and freedoms of individuals. Given the overlap of their respective areas of competence and the lack of statutory provisions establishing an organic framework governing inter-authority relations, the judiciary has been called upon to intervene, establishing the principle of loyal cooperation among such entities. Moreover, the challenges arising from this situation are expected to increase, considering the legislative initiatives undertaken by the European Union to promote and regulate the development of the digital sector; for this reason, legislative or regulatory intervention at both European and national levels becomes imperative, aimed at rationalizing the forms of coordination and interaction among Authorities, in order to provide adequate safeguards for human rights.

Independent Authorities – Loyal cooperation – Constitutionalism – Digital governance

L'Autore è dottore magistrale in giurisprudenza presso l'Università degli Studi Roma Tre e tirocinante presso il Consiglio di Stato

Sommario: 1. Il contesto odierno e l'importanza delle Autorità e di una loro sinergia reciproca. – 2. Un inquadramento (anche costituzionale) delle c.d. Autorità amministrative indipendenti. – 3. La Corte di Giustizia dell'Ue e il principio di leale cooperazione tra Autorità: la sentenza *Meta Platforms e a.* del 4 luglio 2023 quale punto di riferimento per lo svolgimento dei rapporti reciproci tra le Authorities. – 4. L' "inedito" arresto dai toni decisi della giurisprudenza amministrativa italiana: la leale collaborazione tra Autorità indipendenti nella sentenza del Consiglio di Stato n. 497 del 2024. 5. – Gli orizzonti futuri di collaborazione e la necessità di razionalizzare una volta per tutte il dialogo tra le Autorità.

1. Il contesto odierno e l'importanza delle Autorità e di una loro sinergia reciproca

Nell'attuale era digitale, stante l'impetuosa diffusione delle nuove tecnologie[1] nella società, il diritto è chiamato in maniera sempre più urgente a soddisfare quel "bisogno di regolazione dell'informatica" strettamente connesso all'impatto esercitato dai progressi della tecnica sull'esistenza umana individuale e collettiva[2]. Dinanzi alla capacità delle dotazioni tecnologiche, da un lato, di concorrere nel realizzare e nell'implementare le libertà fondamentali dell'individuo, dall'altro, di determinarne gravi restrizioni o violazioni, ci si chiede quale sia il limite entro cui la scienza e la tecnica possano avere un'incidenza sulla sfera fisica, psichica e relazionale della persona senza arrivare a comprometterne la natura[3].

Sicuramente, in passato un quesito del genere ha ricevuto risposta tramite il costituzionalismo moderno, nato col precipuo fine di porre, nell'ottica di garantire la sfera umana, dei freni (giuridici) al potere, a prescindere dalla forma in cui quest'ultimo fosse esercitato[4]. Attualmente, invece, grazie alla Quarta Rivoluzione – caratterizzata dal ruolo sempre più preponderante delle c.d. ICT nell'esistenza di tutti i giorni[5] – viviamo in una "nuova

1. Per una definizione del concetto di "nuove tecnologie" v. Colapietro–Simoncini 2022, p. xv.
2. Così Faini 2020, p. 79 ss.
3. Si pone un interrogativo del genere Cheli 2021, p. 954 (allo stesso modo Faralli 2019, p. 44). In proposito, Resta 2019, p. 200 ss. mostra "chiara consapevolezza della profonda ambiguità di tutti i grandi processi di innovazione tecnologica, capaci di imprimere una netta discontinuità alle dinamiche evolutive della società. Da un lato essi possono avere una valenza fortemente emancipatoria, redistribuendo il potere sociale e creando opportunità di crescita, di progresso e di miglioramento della condizione umana. Dall'altro, se non sono democraticamente governati, rischiano di consolidare le posizioni di privilegio, le disuguaglianze e le asimmetrie di potere esistenti in una data comunità organizzata".
4. In tal senso v. Simoncini 2021, p. 727 ss., il quale sottolinea che "[n]ella prima stagione delle costituzioni ottocentesche, la lesione delle libertà fondamentali veniva essenzialmente dal potere privato, fisico, militare del Re. Nella seconda stagione delle costituzioni post-belliche della metà del Novecento, il potere contro cui proteggere le libertà era quello pubblico, legale dello Stato".
5. Interessanti le riflessioni di Floridi 2017, che nota come sia oggi in atto una profonda rivoluzione culturale, dovuta per lo più alle ICT (le tecnologie dell'informazione e della comunicazione). Queste ultime starebbero trasformando la realtà in una "infosfera sempre più sincronizzata, delocalizzata e correlata", caratterizzata dalla "transizione dall'analogico al digitale e [dal]la crescita esponenziale di spazi informazionali in cui trascorriamo sempre più tempo".

stagione del costituzionalismo", legata a premesse differenti da quelle precedenti e qualificata come stagione del "costituzionalismo digitale"[6].

Questo nuovo tipo di costituzionalismo aspira ad implementare e completare l'armamentario del costituzionalismo tradizionale e si pone quale conseguenza diretta dei mutamenti che la tecnologia ha provocato e provoca tuttora nell'ambito della sfera della persona umana[7]. Il riferimento è al fenomeno dell'"erompere dei poteri privati nei mercati digitali", ossia l'affermazione delle "grandi piattaforme padrone degli algoritmi più intelligenti del mondo" (si pensi, ad esempio, a *Google* o *Meta*), le quali, in virtù della loro "particolare posizione di forza socio-economica" e "in assenza di una qualche forma di 'legittimazione democratica', detengono posizioni di 'potere'" (nel senso che sono in grado di incidere unilateralmente sulla sfera giuridica dei soggetti con cui entrano in contatto)[8] ed esercitano un numero sempre maggiore di funzioni, anche proprie dei pubblici poteri[9].

È in un contesto del genere che si coglie l'importanza del ruolo delle Autorità indipendenti per quanto concerne la tutela delle libertà fondamentali degli individui dinanzi ai rischi originati dall'emersione dei c.d. "poteri privati"[10]. Non a caso le prime "tracce" del nuovo costituzionalismo sono state ravvisate, oltre che sul piano dell'esperienza europea (definita "di natura costituente" e basata sull'impiego del patrimonio delle "tradizioni costituzionali comuni" richiamato dalla Carta di Nizza e già oggetto di interpretazione e applicazione da parte degli organi giurisdizionali nazionali ed europei), anche su quello dell'azione posta in essere dalle Autorità amministrative indipendenti (sia in ambito europeo che interno) a protezione dei diritti fondamentali dell'individuo[11].

In considerazione della portata sovranazionale delle questioni poste dalla "rivoluzione digitale", sarà infatti fondamentale l'attività di tali organismi istituzionali, stante la loro origine e consistenza di "soggetti di natura 'bifronte', collocati sul confine tra le amministrazioni nazionali e l'amministrazione europea"[12]; ad essi il quadro legislativo dell'Unione attribuisce un compito di grande rilevanza, consistente nel garantire in piena autonomia l'attuazione

6. Sul tema del "costituzionalismo digitale" v., *ex multis*, Padovani–Santaniello 2018, Celeste 2019, De Gregorio 2021, Pollicino 2021, Celeste 2022. Secondo Colapietro 2021-b, p. 7 ss., è proprio nell'ottica di tale "nuovo" costituzionalismo che la scienza giuridica deve approcciarsi all'ambiguo rapporto tra diritto e nuove tecnologie, avendo come obiettivo non "quello di inserire la regolazione dei meccanismi automatizzati all'interno delle Costituzioni, quanto piuttosto quello di "plasmare" i sistemi algoritmici per mezzo dei valori costituzionali e della persona". Critico nei confronti della locuzione "costituzionalismo digitale" è, invece, Betzu 2021, p. 188.
7. Sul rinnovato ruolo del diritto costituzionale dinanzi alle sfide della "società algoritmica" cfr. Pollicino 2019 e Pollicino–De Gregorio 2021.
8. Le citazioni sono prese da Cremona, 2021-b. In merito, Scorza 2022, nell'analizzare come si è evoluto Internet, evidenzia che "[a]ll'entusiasmo iniziale di un'*Internet* aperta e libera si è sostituita l'amara constatazione che la dimensione digitale è composta da giardini privati, ciascuno presidiato da pochi grandi soggetti privati". Oggi, infatti, si assiste al fenomeno per cui "una manciata di piattaforme gestite da una manciata di fornitori di servizi privati sono, ormai, divenute autentiche città-Stato nelle quali oltre la metà della popolazione globale vive la propria quotidianità. Ma non siamo cittadini di queste città-Stato, non partecipiamo, attraverso dinamiche democratiche al loro governo, ne siamo semplicemente utenti, ci viviamo in una condizione di libertà condizionata, vincolata, circoscritta e perimetrata per contratto".
9. Cfr. Laviola 2022, p. 27 ss. Sul punto, Simoncini–Cremona 2021, p. 255 notano che "dimensione pubblica e dimensione privata sono oggi profondamente sfidate nella loro storica distinzione; nella pratica della società digitale queste dimensioni sono costantemente mescolate, soggetti privati assumono volontariamente funzioni tradizionalmente proprie dei pubblici poteri, mentre i soggetti pubblici sono spesso costretti a rivolgersi a privati (e non volontariamente li scelgono) per poter continuare ad assolvere le proprie funzioni".
10. Sul fenomeno dei "poteri privati" v. anche Lamberti 2022 e, da un punto di vista prettamente privatistico, Mezzanotte 2018.
11. Cheli 2021, p. 955 ss.
12. Cheli 2016, p. 771.

dei principi eurounitari all'interno degli ordinamenti nazionali, traducendoli in norme regolamentari e in azioni di vigilanza conformi al dettato normativo dell'Ue[13].

Nell'odierna società digitale, però, le Autorità non sono solo organi "bifronte", ma anche entità che – come verrà spiegato più avanti – si avvalgono di un potere diverso dal punto di vista qualitativo rispetto ai tre poteri tradizionali dello Stato, caratterizzato dalla combinazione delle funzioni tipiche statali in vista della messa a disposizione di uno strumento efficiente, adattabile e attrezzato sul piano tecnico per difendere i diritti delle persone rispetto ai nuovi poteri privati. Esse, quindi, ricoprono una posizione sempre più rilevante nella regolazione delle applicazioni pratiche dei mezzi tecnologici, venendo spesso chiamate dal legislatore europeo e da quelli nazionali a controllare il rispetto delle norme relative alle nuove tecnologie[14]. D'altra parte, l'apporto "tecnico" che le Autorità indipendenti possono offrire sul piano regolatorio rende opportuno un loro ampio coinvolgimento nei procedimenti di formazione delle fonti tradizionali, soprattutto laddove si tratti di discipline a elevato contenuto tecnico[15].

In merito a tale profilo, va evidenziato che, anche per quanto concerne gli organismi in questione, sembra sia da preferire l'opzione della c.d. "co-regolazione"[16] (delle attività socioeconomiche delle grandi piattaforme digitali), a metà strada tra la "auto-regolazione" di stampo privato[17]e la "etero-normazione" di matrice pubblica[18]. Si tratta

13. Ne discende che numerose Autorità nazionali operano all'interno di sistemi di controllo istituzionale europeo, delineandosi quali organismi di collegamento tra diritto europeo e diritto interno (cfr. l'intervento in materia di autorità indipendenti della I Commissione affari costituzionali della Presidenza del Consiglio e Interni, in *Atti parlamentari*, Camera dei deputati, XVII legislatura, 14 febbraio 2018).
14. Così Simoncini 2021, p. 731. Pone l'accento sulla necessità che il diritto intervenga per regolare la tecnologia Iannuzzi 2023, p. 92, il quale nota che "uno spazio privo di regolazione ha prodotto concentrazioni enormi di poteri in mano a soggetti privati (*Big Tech*), che ora sono diventati così forti da rendersi impermeabili ad ogni tipo di limitazione tardiva della loro azione e tanto da costringere ad effettuare un'importante riperimetrazione del potere tra soggetti pubblici e privati" (sul tema, Pietrangelo 2023, p. 938 osserva come si sia assistito al passaggio dalla "regolazione dell'opportunità" alla "regolazione difensiva").
15. In questo senso v. Tarli Barbieri 2021, p. 947. Spunti interessanti sul tema sono ricavabili da Iannuzzi 2018 e Iannuzzi 2023.
16. Cfr. Simoncini 2022. V. anche Mobilio 2024.
17. Caratterizzata da un approccio di carattere fortemente liberista, essa concepisce il libero sviluppo del mercato digitale come fattore trainante della crescita economica e del benessere sociale e ammette, quale unica forma di regolazione possibile, l'autoregolamentazione del mercato (Storace 2024, pp. 428 s.) e, quindi, la "delega in bianco alle piattaforme digitali" (Pollicino 2022, p. 1060). Tale "delega", però, comporta che "l'eventuale tutela dei diritti fondamentali si inserisce nelle (e si piega alle) logiche proprie del mercato, del profitto, della pubblicità e della dimensione reputazionale dell'azienda" (Barbareschi 2024, p. 410) e rischia di "offrire alla autoregolazione solo una ulteriore fonte di legittimazione, oltre a quella già molto forte dovuta alla sua effettività" (Frontoni 2024, p. 165). Inoltre, è stato osservato come i tentativi di autoregolazione posti in essere dalle piattaforme abbiano sollevato e sollevino un problema di confusione tra ordine pubblico e ordine privato, avendo l'autoregolamentazione "assunto i caratteri tipici degli strumenti di limitazione del potere, ossia la determinazione di regole e principi generali, il controllo sul rispetto di quelle regole, la costruzione di apparati tendenzialmente indipendenti, chiamati a risolvere eventuali controversie". In tal modo, come già accennato, gli attori del web finiscono per "mimare" i pubblici poteri, compreso un "embrione di principio di divisione dei poteri" (Torchia 2022, p. 1103 ss.), sebbene tutte le funzioni siano articolate e confinate all'interno della piattaforma medesima (per un approfondimento relativo a questi profili cfr. Cremona 2021-a, p. 1262, e Mangiameli 2023, p. 286 ss.).
18. Ponendo l'accento sulla necessità di tutelare i diritti e gli interessi individuali, collettivi e pubblici rispetto ai poteri privati dell'Internet, essa prevede il coinvolgimento del potere pubblico, che si traduce nell'individuazione di una cornice di regole e limiti entro cui si possono muovere le piattaforme online. Come è stato osservato da Mobilio 2020, p. 404 ss., però, "[n]on si può pensare di fare ricorso solamente alla '*hard law*', intesa

di una "forma di regolazione 'ibrida' o 'collaborativa'" in grado di combinare i vantaggi degli altri due approcci (da un lato, la flessibilità e l'adattabilità rispetto al dato tecnologico, dall'altro, la natura vincolante della legislazione) e di limitarne i difetti; mediante essa, si tenta di porre un correttivo alle profonde asimmetrie informative sussistenti tra regolatore e regolato, sia attribuendo alla regolamentazione pubblica il compito di fissare i valori e gli obiettivi generali (ma anche di "vigiliare" sul loro rispetto), sia coinvolgendo i destinatari delle norme (oppure gli organismi o le associazioni rappresentative dei destinatari) nella fase di esecuzione-attuazione[19].

Con specifico riferimento alle Autorità amministrative indipendenti e all'esercizio in concreto dei loro poteri, la "co-regolazione" si pone come soluzione ineludibile a causa dei problemi di "cattura del regolatore" (da parte dei soggetti regolati)[20], i quali inevitabilmente limitano le funzioni normative e sanzionatorie di tali soggetti. Tali problemi, insieme agli effetti prodotti dall'emersione dei poteri privati digitali sul piano della forma di Stato democratica, richiedono l'adozione di modelli di regolazione di tipo misto, proprio in virtù della loro "capacità di coniugare, da un lato, la responsabilizzazione dei gestori delle piattaforme nei confronti della protezione dei diritti individuali, dall'altro, il controllo pubblicistico di carattere sanzionatorio, anche a presidio delle ricadute che le violazioni dei diritti individuali hanno in punto di democraticità dell'ordinamento"[21].

Bisogna poi aggiungere che, attesa l'interazione sempre più marcata – nell'ecosistema digitale – tra la disciplina a tutela dei consumatori, quella a tutela della concorrenza e quella a tutela della privacy (soprattutto con riferimento alla regolamentazione delle grandi piattaforme della Rete)[22], risulta necessaria la messa in campo di una sinergia reciproca tra le Autorità interessate a livello

come regolamentazione ispirata allo schema delle imposizioni assistite da sanzioni ('*command and control*'), che segue una traiettoria di pura eteronomia ('*top-down*'), in cui il destinatario delle norme si vede calata dall'alto una disciplina che può risultare essere ultronea e inadatta alle esigenze del settore. Il rischio complessivo è che metodi e strumenti giuridici tradizionali vengano condannati alla ineffettività, quando non – prendendo in prestito un termine riferito alla tecnologia – ad una sorta di '*disruption*' che ne sancisca il superamento da parte di altre forme di regolazione" (come il mercato o la tecnica). Inoltre, la disciplina della tecnologia da parte del legislatore potrebbe irrigidire troppo il quadro normativo di riferimento, finendo, a causa della sua obsolescenza, per porre un freno all'innovazione digitale e per rendere difficoltoso l'adattamento alle nuove tecnologie (Torchia 2022, p. 1110).

19. Cfr. Simoncini 2022, pp. 1031 e 1045, che nota come alla base di tale "terza via" vi sia la premessa che "la tecnologia digitale sia caratterizzata da un *mix* tale di complessità specialistica e rapidità evolutiva che in molti casi solo i destinatari stessi delle norme sono in possesso delle conoscenze necessarie a svolgere il compito normativo". Per l'Autore, infatti, "il ruolo dei privati, soprattutto delle grandi piattaforme tecnologiche che dominano il mercato dei servizi digitali, è sempre più cruciale nel garantire l'effettività della normazione posta dalle istituzioni pubbliche. Dinanzi a questa tendenza, il modello della co-regolazione rappresenta una sorta di contromisura messa in atto per evitare che questo spostamento non finisca per essere una mera devoluzione di potestà normative ai nuovi 'poteri privati'". In proposito, Pistorio 2024, p. 146 ss. afferma che "[l]'irrompere delle nuove tecnologie e, in particolare, l'evoluzione dei condizionamenti reciproci tra scienza, tecnica e diritto rendono ineluttabile la co-regolazione. Due le ragioni: l'inadeguatezza dell'etero-regolazione pubblica e l'esigenza di porre un freno all'auto-regolazione privata". Da un lato, "l'etero-regolazione non è più sufficiente, né adeguata, soprattutto laddove si tratti di materie tecniche, scientifiche, in continua evoluzione e rispetto alle quali il diritto appare tardigrado e spesso misoneista"; dall'altro, i giganti della Rete "sempre più spesso agiscono con forme di auto-regolazione 'incontrollate', dando vita al c.d. '*far west*' della regolamentazione privatistica".
20. Circa tali problemi cfr. Clarich 2005-a, p. 43 ss.
21. Cardone 2021, pp. 930 e 934.
22. V. Buttarelli 2019.

europeo e interno[23], in modo da proteggere in maniera effettiva i diritti della persona[24] (persona che sempre più spesso viene qualificata, nell'ambiente digitale, come "nuovo 'soggetto debole'", dal momento che si trova a ricoprire allo stesso tempo la posizione di utente, consumatore e interessato del trattamento[25]).

Mentre, però, sia la cooperazione tra Autorità indipendenti appartenenti a Stati membri diversi (preposte alla stessa materia) sia la cooperazione tra Autorità nazionali ed europee risultano sufficientemente strutturate[26], a livello interno, invece, appaiono chiare le criticità che l'assenza di una legge organica sulla collaborazione tra Autorità è in grado di sollevare.

La mancanza di una legge siffatta, infatti, rende particolarmente problematico il riparto di competenze tra Autorità. Spesso accade che "una disciplina settoriale si intersechi (sovrapponga) con altre discipline – che a volte tutelano lo stesso interesse (ponendosi perciò il problema solo in termini di intensità della tutela) a volte, invece, tutelano interessi diversi – con la conseguenza di dovere stabilire come gestire l'*overlapping* e quali siano le Autorità competenti"[27]. Inoltre, all'ingresso di nuove normative europee di tutela del mercato (nella forma, ad esempio, di regolamenti e direttive *self-executing*) si accompagna spesso l'esigenza per il legislatore di individuare l'Autorità competente a vigilare su quel mercato di riferimento e di ripensare le attribuzioni delle *Authorities* già esistenti, rimettendo conseguentemente in discussione il criterio funzionale seguito al momento dell'istituzione di ciascuna. In un quadro del genere, si pongono come necessari, ai fini di un miglior coordinamento nell'esercizio dei poteri delle diverse Autorità, sia interventi del legislatore volti a meglio allineare le varie competenze e ad eliminare alcune incongruenze, sia un maggior impegno delle Autorità stesse a evitare invasioni di campo o duplicazioni

23. Tarli Barbieri 2021, p. 947 afferma la "necessità di una 'regolazione integrata orizzontale' che chiama in causa l'esercizio di poteri normativi a livello interno tra diversi soggetti. Questa esigenza di integrazione orizzontale pone l'esigenza di raccordi anche tra il Parlamento e le diverse autorità indipendenti ma anche tra queste ultime".
24. Come sottolineato da Laviola 2021, p. 207, dinanzi al fenomeno di "patrimonializzazione" dei dati ormai in atto nel mondo digitale (sul quale v., ad esempio, Ricciuto 2019), "il piano della tutela della privacy e quello della protezione del consumatore non sono tra loro in rapporto antinomico, bensì sono necessari l'uno all'altro per garantire una protezione piena alla sfera giuridica del cittadino-consumatore".
25. Così D'Ippolito 2020.
26. Per quanto riguarda la prima tipologia di cooperazione, sono diversi gli esempi di coordinamento tra Autorità nazionali appartenenti a Paesi diversi dell'Ue e competenti nello stesso settore, anche ben funzionanti (basti pensare alla tendenza, documentata anche dalla Relazione annuale del 2023 del GPDP, a ricorrere in maniera sempre più frequente ai "meccanismi di cooperazione e coerenza" tra autorità di controllo istituiti dal Capo vii del Regolamento UE 2016/679). Particolarmente sviluppata risulta anche la cooperazione tra Autorità nazionali ed Autorità e/o organismi dell'Unione (emblematici sono in tal senso i rapporti tra autorità di controllo, da una parte, e Commissione europea e Comitato europeo per la protezione dei dati, dall'altra, in materia di privacy, così come le altre forme di coordinamento esistenti, per esempio, nei settori consumeristico, concorrenziale e delle comunicazioni elettroniche). Diversa, invece, la situazione relativa alla cooperazione tra Autorità nazionali di diversi Paesi europei incaricate della supervisione di materie differenti (per esempio, Autorità per la protezione dei dati e Autorità di regolamentazione e controllo delle telecomunicazioni). Con riferimento a tale collaborazione, non esiste ancora un livello di cooperazione definito; sono infatti assenti nel diritto europeo norme specifiche sui rapporti tra tali organi, motivo per cui l'eventuale cooperazione è ancora su base discrezionale. In realtà, si potrebbe già ricorrere al principio della leale cooperazione di cui all'art. 4, par. 3, TUE e nulla impedirebbe di adottare norme che predispongano strutture funzionali di cooperazione (in modo da rendere la collaborazione un obbligo di legge), ma tutto ciò non si è ancora verificato in concreto. Nonostante ciò, le Autorità dei diversi Paesi europei sembrano intenzionate ad implementare le opportunità di collaborazione reciproca e la recente istituzione da parte dell'EDPB della *Task Force Consumer & Competition* (cfr. *infra*) pare confermarlo.
27. Così Rabitti 2020, p. 83 ss.

di attività (ad esempio, tramite accordi o protocolli di intesa)[28].

Sebbene sia già possibile registrare delle esperienze di cooperazione tra Autorità italiane preposte a materie diverse[29], tale cooperazione non risulta sufficientemente strutturata. Manca, infatti, una normativa che la renda obbligatoria *ex lege*, motivo per cui le collaborazioni sono in larga parte un atto volontario delle Autorità stesse. Emerge la necessità di predisporre strumenti normativi che conferiscano carattere strutturale al coordinamento tra tali soggetti, definendo per esempio forme congiunte di cooperazione (es. *task force*) che possano essere avviate in maniera sistematica e periodica oppure, laddove vi sia la necessità, consentano di deliberare in relazione ad un caso specifico.

Si lega proprio alla situazione di incertezza cagionata da una "lacuna" del genere l'intervento della Corte di Giustizia dell'Unione europea nel caso *Meta Platforms* del 2023, intervento tramite cui la Corte ha cercato di razionalizzare i rapporti tra Autorità per la concorrenza e Autorità per la protezione dei dati personali appartenenti allo stesso Stato membro (in quel caso la Germania)[30]. A tale decisione ha fatto seguito, come si dirà, una rivelante pronuncia del Consiglio di Stato della Repubblica italiana del 2024 (sul caso Telepass), che ha rappresentato il primo vero tentativo da parte del nostro ordinamento di regolare i rapporti tra Autorità indipendenti[31].

2. Un inquadramento (anche costituzionale) delle c.d. Autorità amministrative indipendenti

Volendosi procedere con ordine, sembra opportuno, prima di vedere cosa abbia statuito la giurisprudenza, soffermarsi maggiormente sulle c.d. Autorità amministrative indipendenti. Nate in Italia nell'ultimo quarto del secolo scorso[32], esse si caratterizzano per la "nomina parlamentare e/o governativa di esperti ritenuti al di sopra delle parti e sottratti nel loro agire a vincoli di obbedienza"[33]. Nonostante denominazioni diverse (Commissione, Istituto, Autorità o Garante) e statuti giuridici differenti, nonché la mancanza di una nozione univoca di Autorità indipendente, tutte le Autorità sono infatti connotate da una elevata *expertise* tecnica (collegata alla non-politica)[34], in quanto dirette da persone dotate di adeguate competenze tecnico-professionali e scelte secondo "i più svariati criteri, tutti peraltro rispondenti ad una medesima logica: evitare che i nominati abbiano qualche rapporto con centri di elaborazione dell'indirizzo politico, siano essi partitici, parlamentari o governativi"[35]. Pertanto, gli organismi di cui trattasi sono dotati di indipendenza, "[d]

28. Secondo Clarich 2004, p. 1059, "se si crede nella bontà del modello delle Autorità indipendenti, il coordinamento deve mantenere una dimensione orizzontale tendenzialmente paritaria, sia pur entro una cornice di regole poste che definiscano, distribuiscano e creino i raccordi (sottoforma di pareri, intese, proposte, ecc.) tra le varie competenze. Sarebbe invece incoerente imporre un 'direttore d'orchestra', magari con una connotazione prettamente politica, dotato di poteri di indirizzo".
29. Ad esempio, in applicazione della delibera 309/16/CONS (con la quale l'AGCom ha avviato una indagine conoscitiva su "Piattaforme digitali e sistema dell'informazione") è stato istituito un coordinamento permanente con l'AGCom e il Garante per la privacy, finalizzato a "superare la natura settoriale delle competenze e coniugare i poteri e gli istituti anticoncentrazionistici, regolatori del pluralismo e di tutela della privacy" (così Giannelli 2021, p. 863 ss.). Non si può non menzionare, poi, la "Indagine conoscitiva sui *Big Data*" del 2018, avviata con la delibera n. 217/17/CONS del 30 maggio 2017 e condotta congiuntamente da AGCom, Garante privacy e AGCM.
30. Cfr. *infra* par. 3.
31. Cfr. *infra* par. 4.
32. Sull'origine degli organismi in questione nel nostro ordinamento v., *ex multis*, Cassese 1996-a e Predieri 1997.
33. Così Manetti 2007, p. 5 ss., secondo cui si avrebbe a che fare con "una forma di selezione politica (a differenza di quelle svolte per concorso), ma refrattaria ai criteri dell'appartenenza politica e più in generale della rappresentanza di interessi (sindacali, economici, professionali)".
34. V. D'Alberti 2009, p. 1, che precisa come debbano esserne muniti non soltanto gli uffici, ma anche gli organi verticistici.
35. Merusi–Passaro 2003, p. 7.

alla politica, dal mercato, dalle pressioni dei gruppi d'interesse", essendo necessario che essi possano operare in piena autonomia nei settori ("sensibili") di competenza[36].

Sia la competenza tecnica che l'indipendenza sono strumentali allo svolgimento delle funzioni pubbliche che le Autorità indipendenti sono chiamate a esercitare a tutela di interessi pubblici e privati di rilevanza costituzionale[37]. In particolare, il legislatore italiano affida alle Autorità funzioni diverse, che possono essere sia di regolazione sia tipicamente amministrative (non solo di controllo e vigilanza, ma anche di amministrazione attiva)[38] sia di natura paragiurisdizionale (di risoluzione di controversie tra privati)[39], realizzando in tal modo una singolare concentrazione di funzioni tradizionalmente ripartite tra organi distinti[40]. Nonostante i numerosi tentativi di classificazione operati dalla dottrina – si pensi, ad esempio, alla distinzione tra Autorità di regolazione e di garanzia[41] –, appare dunque difficile individuare una funzione tipica di tali organi[42].

In generale, però, si può evidenziare che alle Autorità vengono quasi sempre assegnate funzioni di regolazione dello specifico settore ordinamentale al quale sono preposte, sia sotto il profilo tecnico che sotto quello organizzativo; regolazione che non sempre si sostanzia in "vere e proprie norme di diritto positivo", ma può concretizzarsi anche in "disposizioni dell'ordinamento settoriale"[43]. Lo strumento principale del potere normativo delle Autorità è costituito infatti dai regolamenti, autorizzati a integrare o persino sostituire interamente la disciplina legislativa[44], ma, in assenza di una simile autorizzazione

36. Così Cerrina Feroni 2023. In merito, v. anche Clarich 2005-b, p. 273.
37. Cirillo–Chieppa 2010, p. 9 ss.
38. Anche nell'ottica di garantire l'efficace svolgimento della funzione di regolazione, la legge assegna alle Autorità funzioni di vigilanza e controllo sul rispetto delle regole fissate, funzioni che si esplicano mediante l'esercizio di poteri amministrativi, di tipo conoscitivo e ispettivo (ad esempio, la possibilità di richiedere informazioni ed esibizione di documenti, disporre accessi, ispezioni e verifiche). Tali poteri sono spesso rafforzati dalla previsione del potere di adottare atti direttamente incidenti su terzi, che irrogano sanzioni amministrative, pecuniarie o interdittive (come la sospensione e la revoca delle autorizzazioni e licenze rilasciate dalle Autorità per l'ingresso nel mercato o per la variazione delle modalità di intervento nello stesso), di cui le Autorità dispongono (insieme a poteri ordinatori o di diffida) per censurare i comportamenti degli operatori che violano le regole di funzionamento del mercato e ripristinare il suo corretto funzionamento.
39. Le Autorità svolgono anche attività di c.d. *adjudication*, le quali si concretizzano in procedimenti di composizione extragiudiziale di controversie sorte fra soggetti operanti nel medesimo settore. Nell'ambito di tali funzioni, la partecipazione dei soggetti interessati ricopre un ruolo fondamentale, non soltanto in vista della relativa tutela nei confronti delle Autorità, quanto soprattutto al fine di garantire la "parità delle armi" fra le parti in contesa, così da garantire, attraverso un contraddittorio "orizzontale" fra queste ultime, l'adozione di decisioni idonee alla soluzione dei conflitti sottoposti alle Autorità (Chieppa 2010, p. 68, definisce le funzioni in questione come "contenziose", in quanto "correlate a situazioni giuridiche di tipo bilaterale orizzontale intercorrenti tra soggetti privati, rispetto alle quali il ruolo delle Autorità è quello di arbitro posto in una posizione neutrale ed equidistante").
40. Così Caretti 2005, p. xii.
41. Spesso si distingue tra Autorità di regolazione (e vigilanza), come la Consob e le Autorità che operano nei servizi pubblici – ossia l'ARERA e l'AGCom –, istituite per assicurare il contraddittorio paritario degli operatori economici in un determinato mercato a tutela degli utenti e dei consumatori (e affidatarie di funzioni in prevalenza normative), e Autorità di garanzia, volte a tutelare i diritti fondamentali della persona. Tuttavia, già Manetti 1999, p. 178 ss. considerava questa distinzione poco convincente sotto il profilo costituzionalistico, ritenendo rilevante, da questo punto di vista, il livello di potere esercitato dalle Autorità, "sub-costituzionale o sub-legislativo".
42. In questo senso v. Cuniberti 2002, p. 4.
43. Malinconico 1996, p. 37.
44. Si è parlato in proposito di una significativa "delega" di potere normativo a questi soggetti da parte del Parlamento per mezzo di leggi apposite, dalla quale sarebbe derivata una "dualizzazione del potere normativo",

del legislatore, gli organismi in questione adottano provvedimenti puntuali (di regolazione dell'attività delle imprese sul mercato), allo stesso modo vincolanti per i relativi destinatari (ad esempio, delibere, raccomandazioni, linee guida, ecc.).

Solo in questo secondo caso verrebbe salvaguardato, perlomeno a livello formale, il principio di subordinazione alle fonti primarie, messo invece in discussione – anche grazie all'autorizzazione legislativa – dall'eventuale adozione di regolamenti da parte delle Autorità indipendenti[45]. Spesso, infatti, il parametro normativo dell'attività delle Autorità risulta talmente connotato da genericità e indeterminatezza che questi organismi devono ininterrottamente arricchire e rendere più preciso il tessuto normativo di cui sono chiamati a garantire il rispetto[46].

Una tale "delega" di potere normativo, a causa della sua ampiezza, è apparsa a molti[47]in contrasto con il principio di legalità sostanziale, il quale richiede la predeterminazione da parte del legislatore degli interessi da realizzare e dei presupposti per l'esercizio dei poteri normativi delegati[48]. Oramai però, soprattutto grazie al lavoro della giurisprudenza amministrativa[49]e costituzionale[50], si ammette pacificamente la legittimità dell'esercizio di poteri normativi da parte delle Autorità indipendenti[51], purché vengano valorizzate "forme di partecipazione procedimentale (c.d. 'contraddittorio orizzontale') volte a garantire la partecipazione dei soggetti interessati con funzione collaborativa e non meramente 'difensiva'" (ad esempio la consultazione preventiva degli interessati)[52].

Superati quindi i dubbi circa la legittimità dell'esercizio di poteri normativi da parte delle Autorità indipendenti, va evidenziato come esse, nonostante il ruolo sempre più rilevante che sono chiamate a svolgere nell'ambito del "costituzionalismo digitale", difettino ancora di un fondamento espresso in Costituzione[53]. Per prima cosa, si deve considerare che le Autorità indipendenti costituiscono nel nostro Paese – e nell'Europa occidentale in generale – "un'esperienza recente, che non ha ancora avuto modo di assestarsi sul terreno costituzionale"[54].

In secondo luogo, questi organismi sono nati in deroga a due principi cardine dello Stato di diritto

in parte conservato dal Parlamento, in parte attribuito ad Autorità indipendenti (Cassese 1996-b, p. 8). Sulle ragioni alla base di tale "delega" cfr. Zammartino 2020, p. 48 ss., secondo cui la "diffusione su vasta scala della facoltà di produrre diritto obiettivo da parte delle diverse autorità amministrative" andrebbe ricollegata al fenomeno del cosiddetto "pluralismo di centri di potere" (sul punto v. anche Bilancia 1999, p. 147).

45. V. Manetti 2007, p. 145 e Cerulli Irelli 2009, p. 2 ss.

46. Così Cuniberti 2002, p. 20. Circa i problemi posti dal tentativo di inquadrare tali poteri nell'ambito del sistema delle fonti cfr. Chieppa 2010, p. 70 e Labriola 1999, p. 14 ss.

47. Cfr., ad esempio, Donati 2017.

48. V. Savino 2001, p. 133, il quale nota come la crisi non colpirebbe invece il principio di legalità formale, dal momento che le Autorità esercitano le funzioni loro attribuite dalla legge.

49. Cfr. Cons. Stato, Sez. VI, sentenza 27 dicembre 2006, n. 7972, e sentenza 20 marzo 2015, n. 1532.

50. Cfr. Corte cost., sent. 7 aprile 2017, n. 69, in *Giur. cost.*, punti 7.1 e 7.2 del Considerato in diritto.

51. Cfr. Cons. Stato, Sez. consult. atti normativi, 14 febbraio 2005, n. 11603/04 (in particolare paragrafi 6.2. e 6.3), parere reso sullo schema di decreto legislativo relativo al Codice delle assicurazioni.

52. Titomanlio 2017, p. 3, il quale ravvisa in tali forme di partecipazione una "peculiare legittimazione delle Autorità".

53. In proposito, si è anche sostenuto che non sarebbe necessario collocare le Autorità indipendenti a livello costituzionale né inserire una esplicita previsione costituzionale, poiché gli artt. 97 e 98 Cost., ponendo l'esigenza di separazione tra politica ed amministrazione, garantirebbero uno spazio per amministrazioni in posizione di relativa indipendenza rispetto all'autorità politica, sottratte, in particolare, all'indirizzo governativo (così Longobardi 2009, p. 102 ss.). Sul punto v. Longo 1996, p. 16 ss., che considera l'istituzione delle Autorità indipendenti il frutto dell'affermazione in Costituzione del principio della separazione, nella sua più avanzata evoluzione "idoneo a configurare l'amministrazione come apparato a sé, separato dal potere politico e regolato direttamente dalla legge".

54. Cheli 2007, p. 1.

di matrice liberale. Innanzitutto, viene derogato il principio di cui agli artt. 95 e 97 Cost. secondo cui "in un governo parlamentare come il nostro l'azione amministrativa deve sempre trovare attraverso il Governo una base di controllo nella sfera parlamentare". Difatti, anche se da tale principio dovrebbe derivare che le Amministrazioni dipendano dall'Esecutivo (a sua volta chiamato a rispondere dinanzi al Parlamento), mediante le Autorità si è delineato un "modello amministrativo 'indipendente' dal Governo"[55], il quale si pone in tensione con il modo tradizionale di intendere il rapporto tra Esecutivo e amministrazione in senso "gerarchico, piramidale"[56].

La seconda deroga, invece, colpisce il principio – che permea il nostro ordinamento costituzionale – di divisione o tripartizione dei poteri, secondo cui la funzione di regolazione è affidata in modo tendenzialmente esclusivo agli organi legislativi, la funzione amministrativa è attribuita all'esecutivo e la funzione giurisdizionale ai giudici (indipendenti tanto dai primi che dal secondo)[57]. Le Autorità indipendenti, come si è visto, si discostano infatti dallo schema della separazione dei poteri, in quanto soggetti che – solitamente – esercitano allo stesso tempo funzioni sia di natura normativa sia di natura amministrativa sia di soluzione delle controversie[58].

Allora, in ragione di queste "due rotture dello schema costituzionale del governo parlamentare"[59], nonché dell'elevato grado di competenza e specializzazione che le caratterizza, molti ritengono che la legittimazione delle Autorità debba ritenersi meramente "tecnocratica", risultando esse estranee rispetto ad un impianto costituzionale fondato sulla sovranità popolare come il nostro[60]. In realtà, la tesi attualmente prevalente è che tali organi dispongano di una forma di legittimazione democratica derivante non già dalla democrazia partecipativa, bensì dalla c.d. "democrazia procedimentale", data dalle sempre crescenti garanzie in termini di trasparenza e di partecipazione ai procedimenti di cui le Autorità sono titolari, delle quali, tuttavia, manca tuttora un disegno coerente e unitario sul piano legislativo[61].

Oltre che ai profili (anche di legittimità costituzionale) di cui si è appena detto, i problemi maggiori per quanto riguarda l'efficacia dell'azione delle Autorità sono legati alla già richiamata questione del riparto di competenze, che risulta difficoltoso,

55. Così Cheli 2013, p. 73.

56. Cfr. Caretti 2005, p. xi. Ne discende un "grave *vulnus* al canone essenziale della responsabilità ministeriale, squilibrando l'assetto dei rapporti fra Governo e Parlamento, proprio del nostro regime parlamentare", con le Autorità che si configurano come "corpi indipendenti rispetto allo stesso Parlamento, al quale in realtà nemmeno rispondono" (Longo 1996, p. 19). Come affermato da Modugno 2019, p. 106, infatti, un tratto peculiare della forma ("mista") di governo parlamentare è proprio il rapporto di fiducia tra Parlamento e Governo, il quale comporta una forma di responsabilità politica del secondo nei confronti del primo (cfr. art. 94 Cost.).

57. Sul principio in oggetto cfr. Modugno 1968.

58. Franchini 1996, p. 71 ss.

59. Cheli 2013, p. 73.

60. Caretti 2005, p. xii. Dinanzi a tali problemi, si è cercato di intervenire direttamente a livello costituzionale, prevedendo una disciplina specifica che consentisse di dirimere le questioni legate alla legittimazione e al fondamento in Costituzione di tali soggetti (cfr. Cuniberti 2002, p. 15, Niccolai 1999, p. 216 e Cheli 2013, p. 71 ss.). A fronte, però, del fallimento di tutti i tentativi di revisione costituzionale, risulta ad oggi ancora assente un riferimento testuale espresso alle Autorità contenuto nella nostra Carta fondamentale. Allora, lo sviluppo piuttosto recente del fenomeno, in mancanza di una precisa cornice costituzionale di riferimento, lascia teoricamente aperta la questione della natura del modello, ma sia la dottrina (*ex multis*, Cuniberti 2002, p. 14 ss. e Passaro 1999, p. 187 ss.) sia la giurisprudenza – tanto civile (cfr. Corte cass., I sez. civile, sent. 30 giugno 2001, n. 8889) quanto amministrativa (cfr., ad esempio, Cons. Stato, Sez. VI, sentenza 29 maggio 2008, n. 2548, punto 11.2.) – sono concordi nel ritenere amministrativa la natura delle Autorità, le quali non configurerebbero pertanto un nuovo potere, a metà strada tra amministrazione, giurisdizione e legislazione, bensì eserciterebbero una funzione amministrativa, diretta alla realizzazione di interessi pubblici (sul tema v. Riviezzo 2005).

61. Groppi–Simoncini 2019, p. 354.

soprattutto a causa della mancanza di previsioni normative che lo disciplinino e dell'eterogeneità propria degli enti di cui trattasi (in termini di composizione, funzioni e poteri). Pertanto, la giurisprudenza è stata costretta ad intervenire, prima a livello europeo (trattandosi di una questione che si pone anche in altri ordinamenti dell'Unione), poi a livello nazionale, per cercare di razionalizzare il dialogo tra *Authorities* dinanzi all'incrocio delle rispettive competenze e attività.

3. La Corte di Giustizia dell'Ue e il principio di leale cooperazione tra Autorità: la sentenza *Meta Platforms e a.* del 4 luglio 2023 quale punto di riferimento per lo svolgimento dei rapporti reciproci tra le Authorities

In relazione alla questione del riparto di competenze, un primo tentativo di chiarimento dei rapporti reciproci tra Autorità nazionali si è avuto con la sentenza della Corte di Giustizia dell'Ue del 4 luglio 2023[62], mediante la quale i Giudici di Lussemburgo si sono espressi sulla domanda di pronuncia pregiudiziale proposta dall'*Oberlandesgericht* di Düsseldorf nell'ambito di un procedimento iniziato il 1° marzo 2016 dal *Bundeskartellamt* (l'Autorità Garante per la concorrenza tedesca) avverso *Facebook* (ora *Meta Platforms*).

Alla base di quella che è stata definita come la "saga" tedesca di *Facebook*[63]si pone la decisione adottata nel 2019 dall'Autorità tedesca della concorrenza[64], che ha utilizzato la disposizione del GWB (la legge tedesca contro le restrizioni della concorrenza) sull'abuso di posizione dominante[65] per vietare i termini contrattuali che *Facebook* impone ai suoi utenti[66], istituendo – in maniera molto simile a quanto fatto in Italia dal Consiglio di Stato nel caso *Facebook*[67] – un collegamento tra

62. Cfr. CGUE, Grande Sezione, sentenza 4 luglio 2023, C-252/21, *Meta platforms e a.* Per un'analisi approfondita della decisione in parola cfr. Bellomo 2024.

63. Van Den Bergh–Weber 2021.

64. Cfr. *Bundeskartellamt*; decisione del 6 febbraio 2019; *Facebook Inc., Menlo Parc*, U.S.A., *Facebook Ireland Ltd., Dubin, Ireland, Facebook Deutschland GmbH/Verbraucherzentrale Bundesverband e. V., Berlin*.

65. Cfr. art. 19, par. 1, GWB.

66. Come sottolineato da Midiri 2021, p. 122, *Facebook* subordina la fruizione del social all'accettazione di un "pacchetto" che prevede l'unione e l'elaborazione dei dati generati usando non soltanto *Facebook* ma anche *WhatsApp* e *Instagram* e consultando i siti terzi (c.d. dati *off Facebook*); dinanzi a tale combinazione forzata, l'utente non ha altra scelta se non quella di prendere o lasciare e dunque finisce per subire una limitazione del diritto all'autodeterminazione informativa. Previsioni contrattuali di questo tipo sono state considerate dal *Bundeskartellamt* come una violazione della legge sulla privacy (in particolare, del RGPD), la quale si sarebbe tradotta – secondo un passaggio "tutt'altro che ovvio" – in abuso di posizione dominante (Pardolesi–Van Den Bergh–Weber 2020, p. 515). Circa i limiti della ricostruzione effettuata dal *Bundeskartellamt*, soprattutto per quanto riguarda il profilo della causalità tra la condotta di *Facebook* e il pregiudizio al mercato, cfr. Davola 2021.

67. Cfr. Cons. Stato, Sez. VI, sentenza 29 marzo 2021, n. 2631. Come evidenziato da Laviola 2022, p. 30 ss., le due vicende si inseriscono nell'ambito del "confronto muscolare in atto a livello mondiale tra *Facebook* e le Autorità Antitrust" e devono essere considerate congiuntamente – nonostante il diverso tipo di violazione contestata dalle Antitrust nazionali (pratiche commerciali scorrette in Italia e abuso di posizione dominante in Germania) e la diversa giurisdizione coinvolta (amministrativa in Italia e civile in Germania) – quali "parti di uno stesso tutto", ovvero il tentativo di arginare il potere delle *Tech Companies* mediante la garanzia del diritto alla concorrenza e del diritto alla protezione dei dati personali (in entrambi i casi, infatti, la disciplina sulla protezione dei dati personali è stata impiegata come parametro per valutare una violazione del diritto della concorrenza). Secondo Pagnanelli 2022, p. 6, nella propria decisione il Consiglio di Stato sembra aver "evitato di pronunciarsi sulla qualificazione giuridica dei dati personali, soffermandosi invece in modo più esteso sul nodo della presunta inapplicabilità della disciplina a tutela del consumatore". In merito, i giudici di Palazzo Spada, lungi dal riconoscere la creazione di "compartimenti stagni di tutela", hanno affermato la "esigenza di garantire 'tutele multilivello' che possano amplificare il livello di garanzia dei diritti delle persone, anche quando un diritto personalissimo sia 'sfruttato' a fini commerciali" (par. 8). Essi, pertanto, hanno ritenuto che la persona debba

la violazione della normativa in materia di privacy e la disciplina antitrust[68].

Con la decisione di cui trattasi, infatti, l'Autorità per la concorrenza tedesca, ritenendo abusive le condizioni generali di contratto applicate da *Facebook* (alla luce della presunta non conformità del trattamento dei dati *off Facebook* da esse previsto ai valori sottesi al Regolamento UE 2016/679) e ravvisando nel trattamento dei dati degli utenti effettuato dalla società uno sfruttamento abusivo della sua posizione dominante sul mercato tedesco delle piattaforme di social media, ha vietato ad essa di subordinare, nelle condizioni generali, l'uso del social network da parte di utenti privati residenti in Germania al trattamento dei loro dati *off Facebook* e di procedere, senza il loro esplicito consenso, al trattamento di tali dati.

Avverso la decisione del *Bundeskartellamt*, *Facebook* ha tempestivamente adito la Corte di appello di Düsseldorf con richiesta di sospensione cautelare (stante la grave minaccia rappresentata dall'ordine comportamentale emesso per il modello di business della società), la quale ha sospeso la decisione con la pronunzia cautelare del 26 agosto 2019[69], a sua volta annullata dal *Bundesgerichtshof* (il Tribunale supremo federale, intervenuto a seguito dell'impugnazione della decisione dell'*Oberlandesgericht* da parte del *Bundeskartellamt*) in data 23 giugno 2020[70]. Il 30 novembre 2020, però, la Corte d'appello di Düsseldorf ha concesso una nuova sospensiva fino all'adozione della sentenza di merito sul ricorso di *Facebook* ed ha deciso di promuovere, ai sensi dell'art. 267 TFUE, rinvio pregiudiziale innanzi alla Corte di Giustizia Ue.

Tra le varie questioni pregiudiziali proposte dall'*Oberlandesgericht*, la Corte ha volutamente affrontato preliminarmente la prima e la settima, in quanto attinenti alla possibilità, *ex* artt. 51 e ss. del RGPD, per un'Autorità nazionale garante della concorrenza di uno Stato membro (quale l'Autorità federale tedesca), di controllare, nell'ambito dell'esercizio di un controllo di abuso di posizione dominante ai sensi del diritto della concorrenza, la conformità di un trattamento di dati personali alle condizioni stabilite nel Regolamento UE 2016/679 (e di eventualmente disporre che l'impresa coinvolta interrompa tale violazione)[71].

Nel trattare tali questioni, i giudici europei hanno subito rilevato che le norme sulla cooperazione previste nel RGPD non sono rivolte alle Autorità nazionali garanti della concorrenza, bensì disciplinano la cooperazione tra le autorità nazionali di controllo interessate e l'autorità di controllo capofila, nonché, eventualmente, la cooperazione di tali autorità con il Comitato europeo per la protezione dei dati e la Commissione europea[72]. In merito, la Corte ha messo in luce l'assenza a livello eurounitario di norme specifiche sulla cooperazione tra un'Autorità nazionale garante della concorrenza e le autorità nazionali di controllo, le quali, come precisato nella pronuncia, esercitano funzioni diverse e perseguono obiettivi e compiti loro propri[73].

A differenza delle autorità di controllo[74], infatti, le Autorità nazionali garanti della concorrenza

essere protetta dal RGPD nella dimensione informativa in senso stretto e dalla disciplina consumeristica nella dimensione commerciale, ponendosi i due plessi normativi in termini di complementarietà (e non di esclusione reciproca) e non determinandosi una sovrapponibilità del regime sanzionatorio tra i due settori, stante la copertura di "ambiti operativi differenti e non contrastanti" (par. 9).

68. In proposito, Laviola 2022, p. 38 ss. evidenzia le assonanze con il caso *Facebook*, ma nota la diversa ricostruzione effettuata dai giudici nelle due vicende.

69. Cfr. *OLG Düsseldorf*; decisione del 26 agosto 2019, *VI-Kart 1/19 (V); Bundeskartellamt c. Facebook*.

70. Cfr. *Bundesgerichtshof*; decisione del 23 giugno 2020; *KVR 69/19*.

71. Le questioni in oggetto sono state sollevate proprio in virtù della circostanza che il *Bundeskartellamt* non avesse esitato a ritenersi competente ad applicare il RGPD nel contesto del controllo del rispetto delle norme antitrust da parte di *Facebook*.

72. Cfr. capo VII del RGPD.

73. Cfr. parr. 42 ss.

74. Incaricate, *ex* art. 51 del RGPD, di vigilare sull'applicazione del Regolamento generale sulla protezione dei dati, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche in relazione al

sono competenti ad adottare decisioni che constatino un abuso di posizione dominante da parte di un'impresa, ai sensi dell'art. 102 del TFUE. Al riguardo, secondo la Corte, la conformità o meno del comportamento dell'impresa in posizione dominante a quanto disposto dal RGPD può rappresentare un importante indizio (fra le circostanze rilevanti del caso specifico) per stabilire se siffatto comportamento costituisca un ricorso a mezzi su cui s'impernia la concorrenza normale, nonché per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori[75].

Preso atto dell'attuale importanza – nell'ambito dell'economia digitale – dell'accesso ai dati personali e del loro sfruttamento[76], la CGUE ha ritenuto inevitabile includere le norme in materia di privacy nel contesto giuridico che le Autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante, anche per evitare di minare l'effettività del diritto concorrenziale all'interno dell'Unione[77]. Allora, laddove un'Autorità nazionale garante della concorrenza ritenga necessario, in occasione di una decisione relativa ad un abuso di posizione dominante, pronunciarsi sulla conformità o meno al RGPD di un trattamento di dati personali effettuato da un'impresa, essa e l'autorità di controllo interessata o, se del caso, l'autorità di controllo capofila "devono cooperare tra loro al fine di garantire un'applicazione coerente" del Regolamento[78].

Nonostante l'assenza nel diritto eurounitario di norme specifiche al riguardo, la Corte di Giustizia ha ritenuto infatti che, quando applicano il RGPD, le diverse Autorità nazionali coinvolte sono tutte vincolate dal principio di leale cooperazione sancito all'art. 4, par. 3, TUE[79], stante il rischio di divergenti interpretazioni del Regolamento. Pertanto, quando l'Autorità garante della concorrenza

trattamento dei dati personali, nonché al fine di agevolare la libera circolazione di questi ultimi all'interno dell'Unione.

75. Cfr. parr. 46 ss. Per la Grande Sezione, nell'esame dell'abuso di posizione dominante di un'impresa su un dato mercato, può risultare necessario che l'Autorità della concorrenza esamini anche la conformità del comportamento dell'impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali appunto le norme in materia di privacy (sul punto v. Pitruzzella 2024, p. v ss., il quale evidenzia come, nell'occuparsi della questione del "rapporto tra il diritto della concorrenza e la regolazione di settore il cui rispetto è affidato ad apposite autorità indipendenti", la Corte si sia distaccata dalle precedenti "prese di posizione secondo cui la regolazione settoriale affidata ad un'autorità indipendente escluderebbe l'*enforcement antitrust*", sostenendo invece che "non solo una violazione delle norme a tutela dei dati personali può essere rilevante per l'accertamento di un abuso di posizione dominante, ma anche la violazione di altri tipi di norme può essere significativa, come potrebbe essere il caso di quelle poste a tutela del consumatore").
76. La disponibilità da parte delle *Big Tech* di un'enorme quantità di dati – forniti, spesso inconsapevolmente, dagli utenti in cambio della fornitura di servizi e/o contenuti digitali (De Franceschi 2019, p. 1389) – avrebbe determinato la nascita di una nuova forma di capitalismo, definita come "capitalismo della sorveglianza", fondata su prassi e meccanismi ben diversi da quelli caratteristici della democrazia di mercato (cfr. Zuboff 2019). I soggetti della Rete, infatti, sono ormai in grado di sfruttare le informazioni "cedute" dagli utenti per arrivare a dedurre le abitudini, i gusti, le preferenze e le opinioni degli individui, con conseguente notevole ritorno economico (Manganelli 2023, p. 883) e inevitabili riflessi antidemocratici, connessi alla profonda asimmetria "conoscitiva" caratterizzante i rapporti tra piattaforme e utenti online (Buttarelli 2019, p. 4).
77. Cfr. parr. 50 ss.
78. Cfr. par. 52.
79. Che dispone così: "In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati". Relativamente a tale principio, la Corte richiama una giurisprudenza costante della stessa (nello specifico, la sentenza della Terza Sezione del 7 novembre 2013, *UPC Nederland BV c. Gemeente Hilversum*, C518/11, punto 59, e quella della Grande Sezione del 1° agosto 2022, *Sea Watch eV c. Ministero delle Infrastrutture e dei Trasporti e a.*, C14/21 e C15/21, punto 156) per affermare che, in forza di esso, "nelle materie rientranti nel diritto dell'Unione, gli Stati membri, ivi incluse le loro autorità amministrative, devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti

è chiamata, nell'esercizio delle proprie competenze, a valutare la conformità del comportamento di un'impresa alle disposizioni in materia di privacy, essa è tenuta a "concertarsi e cooperare lealmente con le autorità nazionali di controllo interessate oppure con l'autorità di controllo capofila; tutte queste autorità sono quindi tenute, in tale contesto, a rispettare i loro rispettivi poteri e competenze, così da rispettare gli obblighi derivanti dal RGPD nonché gli obiettivi di tale regolamento e da preservare il loro effetto utile"[80].

In particolare, alla luce del principio di leale cooperazione, qualora ritenga necessario – nell'ambito del controllo di un abuso di posizione dominante – esaminare la conformità del comportamento di un'impresa alle disposizioni del Regolamento UE 2016/679, l'Autorità nazionale per la concorrenza è tenuta a verificare "se tale comportamento o un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila o, ancora, della Corte". Se così fosse, l'Autorità antitrust non potrebbe discostarsene, pur rimanendo "libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza"[81].

La Corte ha aggiunto anche che, laddove nutra dubbi sulla portata della valutazione effettuata dalle autorità di controllo, laddove il comportamento di cui trattasi o un comportamento simile sia, al contempo, oggetto di esame da parte di tali autorità o, ancora, laddove, in assenza di un'indagine di dette autorità, ritenga che il comportamento attenzionato non sia conforme alle disposizioni del RGPD, l'Autorità per la concorrenza "deve consultare tali autorità e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione"[82].

Di converso, il principio di cui trattasi ha un impatto significativo anche sull'attività delle autorità di controllo. Queste ultime, quando ricevono una richiesta di informazioni o di cooperazione da parte di un'Autorità antitrust, devono rispondere ad essa "entro un termine ragionevole", comunicandole le informazioni a disposizione in grado di consentire di fugare i dubbi sulla portata della valutazione effettuata oppure, se del caso, informandola circa l'intenzione di avviare il procedimento di cooperazione con le altre autorità di controllo interessate o con l'autorità di controllo capofila, al fine di giungere ad una decisione volta a constatare la conformità o meno della condotta al Regolamento. In mancanza di risposta entro un termine ragionevole, l'Autorità della concorrenza "può proseguire la propria indagine", anche qualora "l'autorità nazionale di controllo competente e l'autorità di controllo capofila non sollevino obiezioni a che si prosegua tale indagine senza attendere l'adozione di una loro decisione"[83].

Pertanto, con riferimento alle questioni prima e settima, la Corte ha dichiarato che un'Autorità nazionale competente in materia di concorrenza può constatare, nell'ambito dell'esame di un abuso di posizione dominante di un'impresa, la non conformità al RGPD delle condizioni generali d'uso di essa relative al trattamento dei dati personali,

derivanti dai Trattati, adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, in particolare, agli atti delle istituzioni dell'Unione, nonché astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione" (par. 53).

80. Cfr. par. 54.

81. Cfr. par. 56.

82. Cfr. par. 57. In proposito v. Manzini 2023, p. 202, il quale rileva che "[l]e conseguenze dell'obbligo di leale cooperazione tra autorità appaiono, per quelle competenti in materia di concorrenza, assai stringenti". L'Autore, quindi, si chiede se, in base al suddetto principio, valga anche l'inverso di quanto osservato dalla Corte, cioè se "anche le autorità di controllo della privacy, laddove ritengano che sia necessario esaminare la conformità di un comportamento con il diritto della concorrenza, dovrebbero attivare la procedura di cooperazione in questione". La risposta sembrerebbe per l'Autore positiva, pena la violazione del principio di leale cooperazione e la conseguente annullabilità delle decisioni di tali autorità per "mancanza di conformità con il diritto dell'Unione".

83. Cfr. parr. 57 ss.

purché osservi il suo obbligo di leale cooperazione con le autorità di controllo[84]. Così facendo, la Corte, attraverso l'affermazione del principio – di derivazione europea – di leale cooperazione, ha sottolineato l'indispensabilità della messa in campo di un approccio sinergico da parte delle Autorità nazionali preposte alla tutela della concorrenza, dei consumatori e della privacy, vista la compenetrazione tra le rispettive competenze[85].

4. L'"inedito" arresto dai toni decisi della giurisprudenza amministrativa italiana: la leale collaborazione tra Autorità indipendenti nella sentenza del Consiglio di Stato n. 497 del 2024

In seguito alla pronuncia della CGUE (la quale rappresenta evidentemente un importantissimo punto di riferimento per qualsiasi regolamentazione futura dei rapporti tra *Authorities*), si è mosso in maniera decisa anche il Consiglio di Stato italiano, che nella c.d. "sentenza Telepass"[86] ha evidenziato le difficoltà che possono sorgere quando le competenze delle varie Autorità di settore si sovrappongono e la collaborazione tra di esse non è efficace.

All'origine della decisione in questione si pone il ricorso in appello numero di registro 3363 del 2023, mediante il quale le società *Telepass S.p.a.* e *Telepass Broker S.r.l.* hanno impugnato la sentenza del TAR per il Lazio n. 603 del 2023. Con quest'ultima pronuncia[87], il Tribunale aveva respinto il ricorso proposto da dette società per ottenere l'annullamento del provvedimento adottato dall'AGCM in data 9 marzo 2021 nei loro confronti. Nello specifico, l'Autorità antitrust aveva addebitato alle due società la commissione di una pratica commerciale scorretta (violativa degli artt. 21 e 22, commi 1 e 2, del Codice del consumo) per aver fornito informazioni ingannevoli e/o carenti sulla raccolta e sul trattamento a fini commerciali dei dati degli utenti che richiedevano un preventivo assicurativo relativo a polizze RC Auto attraverso l'app di *Telepass*, nonché sulle modalità di preventivazione e distribuzione dei servizi assicurativi e polizze RC Auto, vietandone la diffusione o continuazione e irrogando una sanzione pecuniaria pari a 2 milioni di euro.

Dinanzi al TAR per il Lazio, allora, le due società, al fine di ottenere l'annullamento del provvedimento sanzionatorio dell'*Antitrust*, hanno contestato, tra l'altro, l'illegittimità del provvedimento per alcune incompatibilità con il Regolamento UE 2016/679 e per aver erroneamente reputato sussistenti i presupposti necessari a configurare una violazione del Codice del consumo[88], per violazione

84. Nel caso specifico, prima di adottare la decisione, il *Bundeskartellamt* aveva contattato – *ex* art. 50 del GWB – il Commissario federale per la protezione dei dati e la libertà d'informazione tedesco, il Commissario di Amburgo per la protezione dei dati e la libertà d'informazione, nonché la *Data Protection Commission* (Autorità per la protezione dei dati irlandese), per informarli del suo intervento. Inoltre, l'Autorità aveva avuto la conferma che tali Autorità non stessero conducendo alcuna indagine riguardo a fatti simili a quelli in causa nel procedimento principale ed esse, a loro volta, non avevano sollevato obiezioni riguardo al suo intervento. Sulla base di ciò, secondo la CGUE, l'Autorità federale garante della concorrenza sembrava aver ottemperato, nel caso in questione, ai suoi obblighi di leale cooperazione con le autorità di controllo nazionali interessate e con l'autorità di controllo capofila.

85. Quanto affermato dalla CGUE in questa decisione è stato recentemente ripreso e sviluppato dal Comitato europeo per la protezione dei dati nel *Position paper on Interplay between data protection and competition law* adottato il 16 gennaio del 2025. In tale documento, il Comitato, sottolineando la sempre più evidente interazione tra diritto in materia di protezione dei dati e diritto della concorrenza (legata, come detto, allo sviluppo dell'economia digitale), ha posto l'accento sulla necessità di implementare la cooperazione tra le Autorità competenti in tali settori, suggerendo la predisposizione, all'interno delle stesse, di "*internal measures*", nello specifico l'istituzione di un'*équipe* dedicata al coordinamento dei compiti di cooperazione e svolgente il ruolo di punto di contatto unico per le altre Autorità.

86. Cfr. Cons. Stato, Sez. VI, sentenza 15 gennaio 2024, n. 497.

87. Cfr. TAR Lazio Roma, Sez. I, sent. 13 gennaio 2023, n. 603.

88. Sul punto, le ricorrenti hanno lamentato l'assenza di un'omissione informativa idonea ad alterare le scelte commerciali del consumatore, essendo stata rispettata la disciplina sulla privacy, ritenuta già di per sé sufficiente e idonea a tutelare il consumatore.

delle competenze e prerogative del Garante privacy, nonché per violazione del principio di leale collaborazione, non essendo stato acquisito il parere di tale Autorità[89].

Occorre segnalare l'avvenuta costituzione nel corso del procedimento di primo grado dell'Autorità garante per la protezione dei dati personali, la quale si è doluta, seppure come circostanza non idonea a compromettere la legittimità della procedura svolta e del provvedimento conclusivo, del proprio mancato coinvolgimento nell'istruttoria sviluppata dall'Antitrust, ritenendo sussistenti tutti i presupposti che deponevano per la necessaria presenza del Garante nel percorso repressivo sanzionatorio dell'AGCM.

Il TAR, con la sentenza n. 603/2023, ha respinto il ricorso delle due società. I giudici amministrativi hanno confermato la sussistenza delle condotte illecite addebitate dall'Autorità Garante della Concorrenza e del Mercato, ma, soprattutto, hanno escluso l'indispensabilità del coinvolgimento del Garante privacy nell'attività repressivo sanzionatoria dell'AGCM, ritenendo che "il collegamento con l'informativa sulla privacy" fosse soltanto "incidentale" e non "dirimente al fine di giudicare della legittimità dei comportamenti contestati". Nella fattispecie, infatti, a rilevare sarebbe stata "l'omissione di informazioni essenziali per consentire ai consumatori il libero e consapevole esercizio delle proprie scelte negoziali, in quanto il piano attinente alla tutela della privacy e, di risulta, la corrispondente competenza del Garante per la protezione dei dati personali costituiscono aspetti del tutto autonomi"[90].

Di conseguenza, secondo il TAR "non sussisteva alcun obbligo di legge di interpellare il Garante", considerato anche che "non si trattava di richiedere un parere obbligatorio nell'ambito di un settore regolato, ai sensi dell'articolo 27, co. 1-*bis*, del Codice del Consumo[91]", essendo il Garante una "autorità generalista preposta alla tutela trasversale di un diritto fondamentale e non un'Autorità regolatoria di settore". Inoltre, secondo il giudice amministrativo, il mancato coinvolgimento del Garante per la privacy non poteva configurare un vizio di istruttoria, vista la totale autonomia dei due piani di tutela[92].

La sentenza di primo grado è stata allora appellata da *Telepass* e *TB*. Tra i motivi di appello dedotti nel secondo grado di giudizio rileva in particolare il terzo, attraverso il quale le ricorrenti hanno lamentato la violazione delle competenze e delle prerogative del Garante della privacy e la violazione dei principi di buon andamento dell'azione amministrativa e di leale collaborazione.

Per le società, la sentenza appellata – come anche il precedente provvedimento dell'AGCM – si sarebbe posta in contrasto con l'art. 27, co. 1-*bis*, del Codice del consumo. Nello specifico, nel corso del procedimento che aveva portato al provvedimento sanzionatorio dell'Antitrust, mentre erano stati ottenuti sia il parere dell'AGCom (ai sensi dell'art. 27, co. 6, del Codice del consumo[93]) sia quello dell'IVASS (ai sensi dell'art. 27, co. 1-*bis*, del

89. Mancata acquisizione che, per le ricorrenti, avrebbe determinato un difetto di istruttoria e una violazione delle regole del procedimento.

90. Cfr. p. 8 del provvedimento del TAR.

91. Cfr. art. 27, co. 1-*bis*, d.lgs. n. 206/2005, così formulato: "Anche nei settori regolati, ai sensi dell'articolo 19, comma 3, la competenza ad intervenire nei confronti delle condotte dei professionisti che integrano una pratica commerciale scorretta, fermo restando il rispetto della regolazione vigente, spetta, in via esclusiva, all'Autorità garante della concorrenza e del mercato, che la esercita in base ai poteri di cui al presente articolo, acquisito il parere dell'Autorità di regolazione competente. Resta ferma la competenza delle Autorità di regolazione ad esercitare i propri poteri nelle ipotesi di violazione della regolazione che non integrino gli estremi di una pratica commerciale scorretta. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione, nel quadro delle rispettive competenze".

92. Cfr. p. 9.

93. Cfr. art. 27, co. 6, d.lgs. n. 206/2005, ai sensi del quale, "[q]uando la pratica commerciale è stata o deve essere diffusa attraverso la stampa periodica o quotidiana ovvero per via radiofonica o televisiva o altro mezzo di telecomunicazione, l'Autorità, prima di provvedere, richiede il parere dell'Autorità per le garanzie nelle comunicazioni".

Codice del Consumo), era mancata l'acquisizione del parere del Garante privacy, nonostante (secondo i ricorrenti) esso fosse necessario in virtù della contestazione di un comportamento anticonsumeristico derivante proprio da una condotta violativa del Codice privacy. Nell'ottica di *Telepass* e *TB*, allora, stante la doverosità del coinvolgimento del Garante (poiché la vicenda riguardava una questione riferibile al trattamento di dati personali), dinanzi alla mancata acquisizione del parere dell'Autorità si aveva a che fare con un deficit procedurale fonte di illegittimità dell'intera procedura e del provvedimento sanzionatorio adottato in conclusione di essa.

Per i motivi appena esplicitati, il Consiglio ha deciso di affrontare preliminarmente la questione del mancato coinvolgimento del Garante privacy nell'istruttoria condotta dall'AGCM, ritenendo che, laddove la relativa censura si fosse rivelata fondata, inevitabilmente sarebbe seguito l'annullamento del provvedimento dell'Antitrust, a prescindere dallo scrutinio degli ulteriori motivi di appello (la valutazione dei quali ne sarebbe stata logicamente assorbita).

In quest'ottica, è necessario evidenziare come nel giudizio di appello, accanto all'AGCM (costituitasi per sostenere l'assoluta infondatezza dei motivi di censura dedotti in appello e la piena correttezza della procedura svolta dall'Antitrust), sia intervenuto anche il GPDP, che ha – per prima cosa – evidenziato la sussistenza di un errore "strutturale" nella sentenza appellata. Ribadendo di essere un'"autorità generalista", infatti, il Garante ha sostenuto che il suo mancato coinvolgimento nella fattispecie in esame – rientrante a pieno titolo nella previsione di cui all'art. 130 del Codice privacy[94] e concernente la "libera circolazione dei dati personali" da chi li ha raccolti verso terzi[95] – rappresentasse un'evidente violazione del principio (dotato di valore costituzionale) di leale collaborazione fra amministrazioni, ai sensi del quale si impone (*erga omnes*) il rispetto del principio di coordinamento delle competenze facenti capo alle diverse Autorità, specie nei casi, non infrequenti, in cui la condotta illecita contestata a soggetti che avrebbero violato discipline settoriali alle quali sono preposte distinte Autorità possa attivare più apparati sanzionatori e dunque plurimi procedimenti di irrogazione.

Nella decisione, il Consiglio ha tenuto a sottolineare "l'intimo collante che lega la contestata condotta (anti)consumeristica imputata alle società *Telepass* e *TB* e il trattamento dei dati personali della clientela". Per il giudice, infatti, l'ampio spettro di ipotesi riconducibili all'attività di trattamento (dei dati) – in virtù dell'ampia definizione contenuta nel RGPD – e quindi ricadenti nella sfera applicativa del Regolamento UE 2016/679, "esclude, già da solo, che la sostenuta (dall'Autorità appellata) esistenza di compartimenti 'stagni', non permeabili tra di loro, tra l'ambito di competenza e dei poteri di AGCM rispetto a quelli di altre Autorità, in particolare del Garante privacy, possa validamente militare nel senso di escludere 'a priori' qualsiasi forma di collaborazione tra le due Autorità nel corso di una indagine che, seppure fondamentalmente indirizzata all'esame circa la compatibilità o meno con la disciplina consumeristica di condotte sviluppate da professionisti, abbia indubitabilmente addentellati forti e robuste caratterizzazioni osmotiche con la tutela dei dati personali, potendosi, *in thesi*, sostenere addirittura una funzionalizzazione tra i comportamenti contestati e la violazione, contemporanea, di discipline normative differenti perché riferite a settori specialistici e quindi la doverosità della cooperazione tra Autorità"[96].

Nello sviluppo del suo ragionamento, il Collegio ha quindi richiamato la sentenza della CGUE risolutiva del caso *Meta Platforms*, ritenendo quanto espresso in essa capace di attagliarsi plasticamente al caso in esame. Per il Consiglio, infatti, la circostanza che il caso posto all'attenzione della CGUE attenesse ad un'ipotesi di abuso di posizione dominante – evidentemente una condotta anticonsumeristica – contestato dall'Autorità antitrust tedesca non impedirebbe di estendere gli approdi raggiunti dalla Corte al caso da decidere, laddove in entrambi emergano "solidi profili di contiguità e di prossimità tra l'indagine dell'Autorità antitrust e il settore della tutela dei dati personali di competenza dell'Autorità di controllo istituita nel Paese

94. Cfr. art. 130 del d.lgs. n. 196/2003, rubricato "Comunicazioni indesiderate".

95. Motivi per cui si tratterebbe di una fattispecie di stretta competenza, tanto in astratto quanto in concreto, del GPDP.

96. Cfr. par. 9.

di riferimento (nel nostro caso il Garante privacy)". Pertanto, i Giudici di Palazzo Spada hanno ritenuto che il mancato coinvolgimento del Garante nel corso dell'istruttoria svolta dall'AGCM costituisse "un deficit procedimentale che infligge al provvedimento finale una connotazione patologica rilevante e tale da necessitare l'annullamento dell'atto sanzionatorio emesso da AGCM a carico delle odierne società appellanti"[97].

In conclusione, il Consiglio, sulla base di quanto detto in precedenza, ha ritenuto fondato il terzo motivo di appello dedotto dai ricorrenti, con conseguente assorbimento dello scrutinio delle ulteriori traiettorie di censura, e ha accolto l'appello delle società, con conseguente riforma della sentenza di primo grado e annullamento del provvedimento emanato dall'Autorità garante della concorrenza e del mercato nei confronti di T*elepass S.p.a.* e *Telepass Broker S.r.l.*

5. Gli orizzonti futuri di collaborazione e la necessità di razionalizzare una volta per tutte il dialogo tra le Autorità

Nelle pagine precedenti si è avuto modo di evidenziare la necessità, ormai impellente nell'odierna economia digitale, che le Autorità nazionali preposte alla protezione dei dati, alla tutela dei consumatori e alla concorrenza ricoprano un ruolo cruciale e sinergico a livello sia nazionale[98] che europeo[99]. Ovviamente, il discorso può e deve

97. Cfr. par. 12. Il Collegio ha evidenziato anche la perfetta consonanza con il precedente reso dalla medesima Sezione nel c.d. caso *Facebook*, di cui ha ripreso la conclusione – confermata dalla CGUE nel caso *Meta Platforms* – secondo cui non è possibile sostenere (come avrebbe voluto fare l'Antitrust) l'esistenza di un'assoluta impermeabilità tra il settore di competenza dell'AGCM (in tema di diritto consumeristico) e quello di competenza del Garante privacy (in tema di protezione dei dati personali), specie nei rapporti tra le Autorità, i quali, in assenza di regole di prevalenza e/o soccombenza delle norme da applicare nelle singole fattispecie, devono essere sempre "ispirati alla più ampia applicazione del principio della leale cooperazione, se non addirittura della fattiva collaborazione". Sul tema dell'*actio finium regundorum* tra AGCM e GPDP in materia di pratiche commerciali scorrette, la VI Sezione è tornata a pronunciarsi di recente con la sentenza n. 80 del 2025, originata dal rigetto, da parte del TAR Lazio, di un ricorso sollevato da Google contro un provvedimento dell'Antitrust (del 2021) con il quale erano state accertate due distinte pratiche poste in essere dalla Società, aventi ad oggetto la raccolta e l'utilizzo, a fini commerciali, dei dati dei propri utenti, sia nella fase di creazione dell'*ID Google*, sia nella fase di accesso ad altri servizi offerti dalla *Big Tech*. I Giudici di Palazzo Spada, di fronte alla doglianza con cui Google aveva sostenuto l'incompetenza (nel caso di specie) dell'Autorità antitrust ritenendo sussistente la competenza trasversale ed esclusiva del Garante, hanno richiamato la precedente giurisprudenza europea e nazionale (compresa la pronuncia sul caso *Facebook*) e, considerato il rapporto di complementarietà tra disciplina del Codice del Consumo e regolazione in materia di privacy, hanno ritenuto che al "criterio della specialità", che vedrebbe prevalere la competenza dell'Autorità di settore, debba essere preferito il "criterio della incompatibilità", che vede possibile l'intervento dell'Autorità settoriale "solo qualora la condotta contestata abbia 'ambiti specifici', nel senso che non rientri nel potere di intervento dell'Antitrust" (par. 2.1.1). In particolare, il Consiglio ha affermato che, "se, da un lato, la normativa sulla privacy ha un carattere trasversale, in quanto relativa ad ogni settore dell'ordinamento, dall'altro, la stessa è posta a tutela dei diritti della personalità, non a tutela della libertà del consumatore, sicché, per quanto attiene alla materia delle pratiche commerciali scorrette, costituisce una normativa settoriale come le altre, con conseguente applicazione del criterio c.d. della incompatibilità sancito inequivocabilmente dal giudice europeo" in tale materia (par. 2.4.3).

98. In questa prospettiva, si spiega la recente proposta del Presidente del Garante Pasquale Stanzione di introdurre nel nostro ordinamento una disciplina sulle forme di cooperazione tra AGCM e Garante per la protezione dei dati personali, che sia speciale rispetto alla previsione di cui all'art. 27, co. 1-*bis*, del Codice del consumo e che miri a realizzare una convergenza effettiva tra tutele consumeristiche e rimedi privacy nonché a massimizzare le garanzie per le persone fisiche, in modo tale da riuscire a governare l'economia delle piattaforme digitali coniugandone esigenza di sviluppo e tutela della persona.

99. A livello unionale, si segnala la recente istituzione da parte dell'EDPB della *Task Force Consumer & Competition* (alla quale partecipa anche il Garante privacy italiano), al fine di aumentare le occasioni di coordinamento in ambito europeo tra le materie oggetto di tutela delle Autorità di protezione dati e quelle di competenza

essere allargato alle altre Autorità amministrative indipendenti (nonché, come si vedrà, alle Agenzie governative), specie per quanto attiene all'ambito del digitale[100], considerate la potenziale sovrapponibilità tra le attività delle diverse *Authorities* e l'opportunità di un approccio convergente e coordinato tra le stesse.

Negli ultimi anni, infatti, la rivoluzione digitale ha spinto il legislatore europeo a emanare una serie di atti normativi derivati, volti a disciplinare i vari "oggetti della società digitale", ossia i dati, le piattaforme, l'Intelligenza artificiale e la sicurezza cibernetica[101]. Ciò ha determinato un "riaccentramento" delle fonti in ambito europeo per la disciplina della tecnologia, finalizzato al "perseguimento dell'indipendenza digitale europea da America e Cina e [a]l bilanciamento tra la *governance* dello sviluppo tecnologico e le esigenze sociali, nel nome dell'affermazione della sovranità digitale europea"[102].

A tale "proliferazione" normativa – volta, sia a garantire uno spazio unico digitale europeo, sia a irrobustire le strutture fisiche della società digitale[103] – si è inevitabilmente accompagnata la predisposizione di una pluralità di Autorità tecniche di settore o, comunque, l'ampliamento dei poteri e delle funzioni delle Autorità già esistenti. Nello specifico, in materia di protezione dei dati personali, si è già rilevato come il RGPD abbia delineato una "trama originale di configurazione e regime delle autorità di controllo e di governo del settore", al cui vertice ha collocato il Comitato europeo per la protezione dei dati personali, il quale rappresenta una "autorità indipendente e di governo della società digitale"[104].

Nel Regolamento (UE) 2022/2065 (*Digital Services Act*) è stato configurato un "sistema a rete", in cui gli Stati membri sono tenuti a designare una o più autorità competenti, incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del Regolamento[105], e, fra esse, il "coordinatore dei servizi digitali", responsabile di tutte le questioni relative alla vigilanza e all'applicazione del Regolamento[106]. Una scelta peculiare effettuata dal DSA riguarda il ruolo attribuito alla Commissione europea nella vigilanza e nell'esecuzione delle norme regolamentari con riferimento ai fornitori di piattaforme online e di motori di ricerca di grandi dimensioni; per lo svolgimento di tale compito,

delle Autorità di tutela della concorrenza e del consumatore. Sul punto v. Gulino 2023, p. 155 ss., che richiama la proposta, avanzata da Giovanni Buttarelli ed attuata negli ultimi anni, di istituire, a livello europeo, una *Digital Clearinghouse* che consenta a tali Autorità di incontrarsi periodicamente per stabilire forme di cooperazione nella *digital economy* (cfr. Buttarelli 2020).

100. Ad esempio, Pitruzzella 2023, p. 25 ss. evidenzia che l'uso dei dati personali da parte delle piattaforme digitali inevitabilmente entra nella sfera di azione di altre Autorità, come l'AGCOM (anche nella prospettiva della maggiore responsabilizzazione delle piattaforme prevista dal *Digital Services Act*) e l'AGCM. Come sottolineato da Calzolaio 2024, p. 104, AGCM, AGCom e Garante privacy "giocano e giocheranno un ruolo, spesso congiuntamente, nel ruolo di autorità di settore applicate alla materia digitale".

101. Per un'approfondita disamina sul punto v. Iannuzzi 2024-b, p. 9 ss.

102. Cfr. Iannuzzi 2021, p. 51.

103. Cfr. Pizzetti 2024.

104. Calzolaio 2024, p. 86 ss., che mette in risalto la diversità di ruolo e funzione del Comitato rispetto all'ENISA, l'autorità indipendente europea operante nel settore della sicurezza cibernetica, la quale, pur esprimendo le migliori e più aggiornate competenze in materia, non si vede attribuite funzioni di governo in senso stretto della materia.

105. Sul punto, v. Orofino 2024-b, p. 165.

106. Cfr. art. 49 del Regolamento (UE) 2022/2065. Nel nostro ordinamento, l'AGCom è stata indicata quale Autorità responsabile dell'*enforcement* del DSA ad opera dell'art. 15 del d.l. n. 123/2023 (convertito con modificazioni dalla legge n. 159/2023), in attuazione dell'art. 49, par. 2, del Regolamento di cui sopra. Ai sensi del co. 2 dell'art. 15 del d.l. n. 123/2023, l'AGCM, il Garante privacy e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'AGCom delle funzioni di Coordinatore dei Servizi Digitali. A tale scopo, le Autorità "possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione".

infatti, sono stati conferiti alla Commissione gli stessi poteri attribuiti alle Autorità nazionali relativamente agli altri fornitori di servizi di intermediazione (ossia poteri di indagine sul rispetto degli obblighi regolamentari, il potere di avviare un procedimento laddove vi sia il sospetto della violazione di un obbligo, poteri di audizione e di raccolta di informazioni, poteri ispettivi e correttivi, anche sanzionatori)[107].

Diverso, invece, è il sistema disegnato dal Regolamento (UE) 2022/1925 (*Digital Markets Act*), il quale ha previsto che i poteri sanzionatori e di vigilanza siano accentrati in capo alla Commissione, che rappresenta l'autorità preposta al controllo di tale Regolamento[108], poiché reputata la sola in grado di "tenere testa" ai c.d. *gatekeeper*[109]. Pertanto, il ruolo delle Autorità nazionali e degli Stati nell'*enforcement* del DMA risulta assai limitato[110].

Per quanto riguarda poi il Regolamento (UE) 2022/868 (*Data Governance Act*), va specificato che, ai sensi di tale atto, la Commissione ha i poteri caratteristici di un'"autorità amministrativa di governo" e si avvale di un Comitato europeo per l'innovazione in materia di dati[111]. In tale assetto, ad essere competenti in materia di vigilanza e controllo sono le Autorità nazionali designate dagli Stati membri, ossia le "Autorità competenti per i servizi di intermediazione dei dati" e le "Autorità competenti per la registrazione di organizzazioni per l'altruismo dei dati"[112]. In Italia, è stato recentemente approvato dal Consiglio dei Ministri, in esame preliminare, il decreto legislativo di adeguamento della normativa nazionale alle disposizioni di tale Regolamento, che ha designato l'Agenzia per l'Italia Digitale (AgID) come "autorità responsabile per lo svolgimento dei compiti relativi alla procedura di notifica per i servizi di intermediazione dati nonché quale autorità competente alla registrazione di organizzazioni per l'altruismo dei dati"[113].

In maniera simile a quanto appena visto con riferimento al *DGA*, nel Regolamento (UE) 2023/2854 (*Data Act*) è stato previsto l'obbligo in capo agli Stati membri di designare una o più "Autorità competenti", incaricate dell'applicazione e dell'esecuzione del Regolamento, istituendole *ex novo* o facendo affidamento sulle Autorità esistenti. La normativa in questione ha poi prescritto che, nel caso in cui uno Stato membro designi più di un'Autorità competente, esso sia tenuto a designare (tra esse) un "coordinatore dei dati", con il compito di facilitare la cooperazione tra le Autorità competenti e di assistere le entità che rientrano nell'ambito di

107. Cfr. artt. 65 e 66 del DSA.

108. Cfr. considerando 91 del DMA.

109. Per la definizione di *gatekeeper* v. Midiri 2021, p. 111.

110. In tal senso v. Orofino 2024-a, p. 193 ss. In proposito, Torchia 2022, p. 1107 ss. osserva come si abbia a che fare con "un assetto dei poteri di vigilanza, controllo e sanzione fortemente centralizzato in capo alla Commissione, in misura certamente maggiore rispetto all'assetto oggi vigente per la tutela della disciplina della concorrenza. Le ragioni di questa scelta sembrano potersi trovare per un verso nella novità delle regole – con l'introduzione di misure regolatorie *ex ante* in genere applicate dalle autorità di regolazione ma non dalle autorità antitrust – che in assenza di una esperienza consolidata potrebbe portare a dispersione, frammentazione ed esiti incoerenti nell'applicazione, e per altro verso nell'esigenza di non consentire dislivelli regolatori nel mercato unico digitale europeo".

111. Cfr. art. 29 del DGA. Sulle criticità sollevate dal Comitato v. Iannuzzi 2024-a, p. 122, il quale, alla luce dei compiti assegnati a tale organismo dall'art. 30 del DGA, evidenzia il rischio di sovrapposizioni con le funzioni del Garante europeo e del Comitato europeo.

112. Cfr. sia l'art. 13 sia l'art. 23 del DGA, che prevedono l'istituzione, da parte di ciascuno Stato membro, di una o più Autorità di questo tipo. Per quanto riguarda i loro compiti di monitoraggio e controllo della conformità (alle norme regolamentari), cfr., rispettivamente, gli artt. 14 e 24 del DGA.

113. Cfr. Comunicato stampa del Consiglio dei ministri n. 88, 3 luglio 2024. Evidentemente, il legislatore nazionale ha optato per attribuire le funzioni di cui trattasi alla stessa Autorità (possibilità prevista dal co. 1 dell'art. 26 del DGA), avvalendosi di un organo già esistente (appunto, l'AgID).

applicazione del Regolamento su tutte le questioni relative alla sua applicazione ed esecuzione[114].

I problemi principali, però, sono senza dubbio generati dal Regolamento europeo sull'intelligenza artificiale (Regolamento UE 2024/1689), che, al fine di sovrintendere e vigilare sulla corretta applicazione della normativa regolamentare, ha istituito "diversi livelli di 'governance', sia a livello sovranazionale che nazionale"[115]. Al primo livello, si trovano l'Ufficio per l'IA, ossia la "funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA"[116], e il Consiglio per l'IA, che agevola la coerenza e il coordinamento tra le Autorità nazionali competenti per quanto riguarda l'attuazione del Regolamento e, in cooperazione con le Autorità di vigilanza del mercato interessate e previo accordo di queste ultime, sostiene le attività congiunte delle Autorità di vigilanza del mercato[117].

Quanto al livello nazionale, l'art. 70 del Regolamento prevede che ogni Stato membro istituisca o designi come "autorità nazionali competenti" almeno una "autorità di notifica" e almeno una "autorità di vigilanza del mercato". Nel nostro ordinamento, per il tramite del disegno di legge n. 1146 recante "Disposizioni e delega al Governo in materia di intelligenza artificiale", approvato dal Consiglio dei ministri il 23 aprile 2024 (e oggi ancora all'esame del Senato), si è deciso di identificare quali Autorità nazionali per l'intelligenza artificiale l'AgID e l'Agenzia per la cybersicurezza nazionale (ACN), alle quali è stato affidato il compito di "garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale" e di "assicura[re] l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di Intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea" (art. 18, co. 1), mantenendo però "ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali" (co. 3)[118].

Da quanto detto sino ad ora emergono chiaramente le criticità poste dai recenti interventi

114. Si segnala un ruolo di rilievo anche delle autorità di controllo, incaricate di sorvegliare l'applicazione del *Data Act* per quanto concerne la protezione dei dati personali, e del Garante europeo della protezione dei dati, incaricato di monitorare l'applicazione del Regolamento nella misura in cui riguarda la Commissione, la Banca centrale europea o gli organismi dell'Unione. Sul punto v. Iannuzzi 2024-a, p. 127 ss., che precisa come l'applicazione coerente delle norme regolamentari sia affidata al Comitato europeo per l'innovazione dei dati, che fornirà assistenza e consulenza alla Commissione europea nello svolgimento dei compiti inerenti a tale Regolamento.

115. Espressione impiegata da Colapietro 2022, p. 8 con riferimento alla Proposta di regolamento sull'intelligenza artificiale.

116. Cfr. art. 3, n. 47, dell'*AI Act*. Attraverso esso, la "Commissione sviluppa le competenze e le capacità dell'Unione nel settore dell'IA" (cfr. art. 64 dell'*AI Act*).

117. Cfr. artt. 65 e 66 dell'*AI Act*. Completano il sistema di governance a livello europeo un forum consultivo e un gruppo di esperti scientifici indipendenti. Il primo ha il compito di fornire consulenza e competenze tecniche al Comitato e alla Commissione tramite pareri, raccomandazioni e contributi scritti (cfr. art. 67 dell'*AI Act*); il secondo dovrà sostenere le attività di esecuzione previste dal Regolamento europeo, fornendo in particolare consulenza e sostegno all'Ufficio per l'IA e agli Stati membri (cfr. artt. 68 e 69 dell'*AI Act*).

118. In Italia, si è quindi voluto affidare il ruolo di controllo sull'IA a organi governativi, piuttosto che a un organo terzo e indipendente, quale un'Autorità amministrativa indipendente. L'AgID e l'ACN, infatti, pur essendo autorità dalla spiccata caratura tecnica, per il fatto di gestire interessi e attività di rilevanza strategica, sono collocate nell'alveo del potere esecutivo, che le indirizza e governa (Calzolaio 2024, p. 100 ss.). Questa scelta ha suscitato la reazione poco entusiasta, sia del Garante privacy, che, il 2 agosto 2024, nel dare il proprio parere favorevole allo schema di disegno di legge, ha chiesto al Governo di integrarlo in più parti, in modo tale da garantire una maggiore tutela dei dati personali dei cittadini, prevendendo un coinvolgimento ed una partecipazione più attiva del Garante stesso, quale autorità preposta alla protezione dei dati (costantemente coinvolti nei sistemi di intelligenza artificiale); sia della Commissione europea, che ha inviato – il 5 novembre 2024 – un

effettuati dal legislatore europeo nel tentativo di regolare i fenomeni digitali. Un modello di questo genere, infatti, ha inevitabilmente innescato un processo di moltiplicazione delle competenze assegnate, sempre più numerose ed estese, che spesso si intersecano e si sovrappongono, con conseguenti problemi nella ripartizione delle stesse[119]. Allora, è necessario che l'assegnazione delle competenze sia chiara (facilmente riconoscibile) e specifica, ovvero indicata in modo preciso e coerente con le finalità sottostanti l'istituzione dell'Autorità[120]. Emerge la necessità di avviare un adeguato processo di integrazione delle attività delle *Authorities* e di ripensare l'attuale modello di articolazione delle attività e dei compiti di tali organismi, promuovendo nuovi modelli di convergenza improntati alla cooperazione e all'efficientamento[121].

In una situazione del genere, piuttosto che una fusione tra differenti *Authorities* finalizzata a istituire un'Autorità unica di regolazione, appare necessario ed opportuno (per tenere testa ai colossi del Web) un più intenso coordinamento tra le stesse (e, ormai, anche le Agenzia governative) negli interventi che interessano i mercati digitali, facendo in modo che alla convergenza e interdipendenza tra spazio fisico e digitale caratteristiche della Quarta Rivoluzione si accompagni una corrispondente convergenza di intenti tra Autorità[122]. Solo attraverso una serrata e costante collaborazione tra i diversi enti caso per caso coinvolti, tale da consentire l'applicazione congiunta delle normative che vengano in considerazione e la messa in campo delle competenze di più specialisti, sarà allora possibile garantire effettivamente la sfera delle libertà della persona, sempre più in pericolo e a rischio nell'attuale era digitale[123].

I vantaggi di un'integrazione degli "asset" delle Autorità sarebbero sicuramente un risparmio di risorse, l'accentramento presso un unico organismo dei rispettivi compiti istituzionali, nonché la predisposizione di competenze convergenti ed aggiornate; tuttavia, la difesa del cittadino-utente

parere circostanziato all'Italia, con cui ha espresso i suoi dubbi sull'autonomia e sull'imparzialità di queste due Agenzie, mettendo in luce come una scelta quale quella del Governo Meloni rischi di minare la credibilità della supervisione italiana sull'IA e di compromettere l'efficacia della normativa nazionale in un settore così delicato.

119. Iannuzzi 2024-b, p. 30 intravede "un profilo critico nella proliferazione e nella frammentazione dei poteri di intervento delle diverse Autorità indipendenti, nazionali ed europee, e delle varie Agenzie di governo, chiamate a garantire l'osservanza dei diversi atti normativi derivati dell'Ue, a fronte del rischio di rendere interpretazioni diverse del medesimo principio".

120. Di fronte all'incertezza dei confini tra un'Autorità e l'altra, Panetta 2024 arriva a proporre l'istituzione di "una grande Autorità tecnologica, il Garante dei Dati e dell'AI", pure per "semplificare la vita delle aziende che diversamente vedranno moltiplicarsi il numero dei regolatori e dei controllori". Come sottolineato dall'Autore, infatti, "il numero dei soggetti delegati e competenti in materia non si limiterà alle sole Agid, Acn e Garante Privacy – sopra tutte e come è naturale – ma anche l'Agcom e l'Antitrust avranno poteri e voce da far sentire nei loro mercati di riferimento".

121. Già Pagnanelli 2021, p. 805 aveva ravvisato il rischio che, con il moltiplicarsi di soggetti dotati di poteri regolatori, di consulenza e controllo, si producesse, "nel tentativo di meglio regolare e meglio tutelare, l'effetto contrario di aumentare e irrigidire le procedure, a scapito della efficienza del mercato unico, della sicurezza, e della tutela dei diritti".

122. In questo senso v. De Minico 2021, p. 981 ss., che, nel riflettere su come strutturare il dialogo tra le Autorità (nello specifico, tra AGCM e Garante privacy), si esprime negativamente sulla creazione di un'Autorità indipendente per la rete. Per l'Autrice il problema non risiederebbe nel "vuoto istituzionale" (colmabile tramite una "autorità *ad hoc*"), bensì nel "mancato coordinamento tra i soggetti esistenti".

123. In merito cfr. Faini 2023, p. 403 ss. e Battelli 2022, p. 25 s. Come evidenziato da Colapietro 2021-a, p. 835, dinanzi alla rapida ed incessante evoluzione delle tecnologie, le Autorità stanno provando a "trovare nuove sinergie al fine di offrire punti di riferimento comuni" (come dimostrato dalla già citata "Indagine conoscitiva sui *Big Data*"), ma "la strada della cooperazione tra le *Authorities* rischia di essere molto lunga e tortuosa e occorrerà del tempo affinché il lavoro condiviso possa cominciare a dare qualche frutto che possa giungere a maturazione".

dinanzi alle complessità del mondo digitale non sembra poter prescindere da un'azione coordinata dei vari soggetti istituzionali competenti, la cui efficacia nei confronti delle piattaforme globali risulta inevitabilmente rafforzata dalla possibilità di irrogare rilevanti sanzioni pecuniarie e di esercitare i diversi poteri prescrittivi ed inibitori attribuiti (ad essi) dalla legge[124].

Ad un intervento di questo tipo si frappone, però, la persistente assenza nel nostro ordinamento di uno statuto generale delle Autorità indipendenti che contenga norme di coordinamento e che sia tale da rendere la cooperazione un obbligo di legge[125]. In attesa di regolazione – la quale potrà avvenire, oltre che attraverso una legge generale che disciplini i rapporti tra i soggetti in questione, anche tramite regolamenti delle singole Autorità –, fino a questo momento l'interlocuzione nei casi concreti si è svolta spesso in via informale.

Sicuramente, il fatto che in questi anni le Autorità italiane abbiano sottoscritto numerosi protocolli di intesa e accordi di collaborazione nello svolgimento delle rispettive funzioni istituzionali è positivo[126]. In essi viene spesso sottolineata, stante la convergenza di interessi dovuta all'esercizio di funzioni complementari, l'opportunità di instaurare, nel rispetto dell'autonomia e dell'indipendenza dei relativi compiti, rapporti di collaborazione tra le due Autorità interessate, così da coordinare e rendere più efficace l'esecuzione dei rispettivi mandati. Molte volte, poi, viene precisato che la cooperazione ivi contemplata si inserisce nell'ambito di un più generale principio di leale collaborazione tra pubbliche istituzioni[127], che rende necessario condividere le informazioni e i dati acquisiti nell'esercizio delle relative funzioni, in coerenza con i principi di imparzialità e buon andamento dell'azione amministrativa di cui all'art. 97 Cost. e nei limiti dei rispettivi ordinamenti.

Tuttavia, considerata anche la natura di atti di *soft law* dei protocolli di intesa e la conseguente mancanza di efficacia vincolante diretta[128], permangono i problemi pratici che l'assenza di una legge organica sulla cooperazione tra Autorità è in grado di provocare, essendo di fatto rimesso al "buon cuore" di chi gestisce volta per volta l'istruttoria il coinvolgimento di questa o quella Autorità[129].

Un'esperienza da cui trarre ispirazione potrebbe essere quella francese, dove la legge 2017-55 del 20 gennaio 2017, recante lo statuto generale delle autorità amministrative indipendenti e delle autorità pubbliche indipendenti, permette alle *Autorités administratives indépendantes* di cooperare in un quadro formale, ad esempio, attraverso la richiesta di pareri[130]; in più, oltre al ricorso ai meccanismi

124. Spunti in questo senso sono ricavabili da Bolognini 2019, secondo cui oggi sembra opportuno optare per "una forma di 'immanenza sostanziale' delle tutele giuridiche", piuttosto che per "una convergenza esterna tra iverse competenze di distinte autorità".

125. A livello generale, infatti, l'art. 15 della l. n. 241/1990 si limita ad affermare che "le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune".

126. Si pensi, tra gli altri, ai Protocolli d'intesa stipulati tra AGCM e IVASS nel 2014; tra AGCM e AGCom nel 2016; tra ANAC e Garante privacy nel 2019; tra Garante privacy e ACN nel 2022 (espressione, in realtà, dell'ormai inevitabile collaborazione tra Autorità indipendenti e Agenzie governative); tra AGCom e Garante privacy nel 2023; tra ANAC e AGCM nel 2024.

127. Principio che trova riscontro, ad esempio, per il Garante privacy, nell'art. 154, co. 4, del d.lgs. n. 196 del 2003, che si limita a disporre che "il Garante collabora con altre autorità amministrative indipendenti nazionali nello svolgimento dei rispettivi compiti".

128. Ruotolo 2020, p. 107.

129. Emblematica sulla questione la vicenda *Telepass* (v. *supra*).

130. Cfr. art. 15 dello statuto, ai sensi del quale "an independent administrative authority or an independent public authority may refer to another authority for an opinion on any matter falling within the latter's competence". Per quanto attiene, nello specifico, alla cooperazione tra l'*Autorité de la concurrence* e la *Commission Nationale de l'Informatique et des Libertés* (CNIL), cfr. l'art. R463-9 del Codice di commercio francese. Un'occasione importante in cui l'*Autorité de la concurrence* ha potuto beneficiare di un parere emesso dalla CNIL su

legislativi formalmente esistenti, le Autorità francesi possono consultarsi su base informale, tramite scambi di opinioni su una determinata questione oppure per preparare una richiesta formale, e, a tal fine, instaurano contatti regolari.

In tale contesto di cooperazione, ad esempio, l'*Autorité de la concurrence* e la CNIL hanno firmato una dichiarazione congiunta nel 2023[131], con lo scopo di affrontare insieme le questioni poste dall'interazione tra il diritto della concorrenza e la protezione dei dati personali e di rafforzare "*their already long-standing cooperation*" al servizio delle imprese e degli utenti[132], anche nell'ottica di sviluppare la prevedibilità e la coerenza delle loro azioni (in modo tale da favorire la concorrenza e scoraggiare comportamenti anticoncorrenziali o lesivi della privacy)[133].

L'auspicio, allora, è che, anche in Italia, prendendo magari spunto da esperienze rivelatesi "vincenti" (come quella francese), il legislatore e/o le Autorità indipendenti si attivino concretamente per regolare in modo sistematico e organico la collaborazione tra queste ultime, ad esempio, istituendo "procedure di raccordo" che consentano l'innesto, nell'ambito del procedimento principale o comunque precedentemente avviato, di un accertamento incidentale, con eventuale esito prescrittivo, o anche solo di una mera pronuncia consultiva da parte dell'altra Autorità.

In questo modo verrebbero implementate significativamente le garanzie per la sfera personale degli individui, i quali risulterebbero così liberati dall'attuale stato di incertezza circa la precisa individuazione degli organismi sul cui intervento poter fare affidamento nelle varie situazioni che dovessero prospettarsi in concreto. Inoltre, l'azione degli organi deputati alla governance del digitale si rivelerebbe più efficace, efficiente e ponderata, a evidente giovamento della protezione dei diritti e delle libertà delle persone in rapporto ai rischi sempre più insidiosi del mondo "digitalizzato".

Riferimenti bibliografici

S. Barbareschi (2024), *Alla ricerca della fonte di regolazione della giustizia consensuale digitale. Il caso delle* Online Dispute Resolution, in "Osservatorio sulle fonti", 2024, n. 1

E. Battelli (2022), *Negoziabilità dei dati personali e modelli di valorizzazione economica*, in "Rivista di diritto dell'impresa", 2022, n. 1

questioni relative all'applicazione della normativa in materia di protezione dei dati personali è rappresentata dal caso *Apple ATT* (2021), che ha visto l'Autorità francese garante della concorrenza collaborare con la CNIL per valutare la legittimità della modifica di *Apple* introduttiva del sistema *App Tracking Transparency* (ATT) sotto il profilo della privacy degli utenti.

131. Cfr. *Competition and personal data: a common ambition, Joint declaration by the Autorité de la concurrence and the Commission nationale de l'informatique et des libertés* (CNIL), 12 dicembre 2023.

132. Nella dichiarazione congiunta, il caso *Apple ATT* viene richiamato, insieme al caso *GDF Suez* (cfr. *Decision 14-MC-02 of 9 September 2014 regarding a request for interim measures submitted by Direct Energie in the gas and electricity sectors*), quale esempio di occasione in cui l'Antitrust francese ha sollecitato l'intervento del Garante privacy francese su questioni concernenti l'applicazione della normativa in materia di protezione dei dati personali. Come esempio di caso inverso, invece, viene indicata la richiesta formale indirizzata nel marzo 2023 dalla CNIL all'*Autorité de la concurrence* per "an opinion on draft recommendations for mobile applications, designed to clarify the obligations of the different players in this sector with regard to protection of personal data regulations".

133. Stante la compatibilità dei rispettivi "public policy objectives", le due Autorità, guardando anche alla sentenza resa dalla CGUE nel caso *Meta Platforms*, hanno deciso di sfruttare in maniera più consistente le sinergie normative esistenti e di impegnarsi a consultarsi reciprocamente (laddove necessario), a sviluppare una migliore comprensione dei rispettivi "legal frameworks" (così da essere in grado di individuare meglio le questioni che richiedono un approccio congiunto), a prendere in considerazione studi congiunti su temi di interesse reciproco, a scambiare personale e a organizzare riunioni periodiche.

G. Bellomo (2024), *La Grande Sezione interviene sul principio di leale cooperazione tra autorità garanti e sul principio di liceità dei trattamenti di dati personali attuato da Facebook*, in "DPCE online", 2024, n. 1

M. Betzu (2021), *Poteri pubblici e poteri privati nel mondo digitale*, in "Rivista Gruppo di Pisa", 2021, n. 2

P. Bilancia (1999), *Attività normativa delle autorità indipendenti e sistema delle fonti*, in S. Labriola (a cura di), "Le autorità indipendenti. Da fattori evolutivi ad elementi della transizione nel diritto pubblico italiano", Giuffrè, 1999

L. Bolognini (2019), *Intervista* (di M. Fiordalisi), in "Corriere delle comunicazioni", 2019

G. Buttarelli (2019), *This is Not an Article on Data Protection and Competition Law*, in "Competition Policy International", 25 February 2019

G. Buttarelli (2016), *Big Data and Digital Clearing House*, in "edps.europa.eu", 2016

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

A. Cardone (2021), *Brevi note di sintesi sulla distinzione tra misure individuali e decisioni politiche nella regolazione degli algoritmi e nella definizione dei poteri delle Autorità garanti*, in "Osservatorio sulle fonti", 2021, n. 2

P. Caretti (2005), *Introduzione*, in Id. (a cura di), "Osservatorio sulle fonti 2003-2004. I poteri normativi delle autorità indipendenti", Giappichelli, 2005

S. Cassese (1996-a), *Le autorità indipendenti: origini storiche e problemi odierni*, in S. Cassese, C. Franchini (a cura di), "I garanti delle regole", il Mulino, 1996

S. Cassese (1996-b), *Poteri indipendenti, Stati, relazioni ultrastatali*, in "Il Foro Italiano", vol. 119, 1996, n. 1

E. Celeste (2022), *Digital Constitutionalism. The Role of Internet Bills of Rights*, Routledge, 2022

E. Celeste (2019), *Digital Constitutionalism: A New Systematic Theorisation*, in "International Review of Law, Computers & Technology", vol. 33, 2019, n. 1

G. Cerrina Feroni (2023), *Riflessioni sul concetto di indipendenza*, intervento in occasione della presentazione del volume "La privacy dell'era digitale – Le Relazioni dei Presidenti dell'Autorità Garante 1997-2022" (a cura di P. Stanzione), Roma, 22 febbraio 2023

V. Cerulli Irelli (2009), *Sul potere normativo delle Autorità amministrative indipendenti*, in "astrid.eu", 2009

E. Cheli (2021), *Conclusioni*, in "Osservatorio sulle fonti", 2021, n. 2

E. Cheli (2016), *Due indispensabili premesse al dibattito*, in F. Lanchester (a cura di), "Parlamenti nazionali e Unione Europea nella governance multilivello. Atti del convegno, Roma-Camera dei Deputati, 12-13 maggio 2015", Giuffrè, 2016

E. Cheli (2013), *L'esperienza italiana delle autorità amministrative indipendenti*, in "Associazione per gli studi e le ricerche parlamentari", Giappichelli, 2013, quad. n. 22

E. Cheli (2007), *L'innesto costituzionale delle Autorità indipendenti: problemi e conseguenze*, in "Astrid Rassegna", 2007, n. 7

R. Chieppa (2010), *Poteri esercitati, procedimento e contraddittorio davanti alle autorità indipendenti*, in G.P. Cirillo, R. Chieppa (a cura di), "Le autorità amministrative indipendenti", Cedam, 2010

G.P. Cirillo, R. Chieppa (2010), *Introduzione*, in Id. (a cura di), "Le autorità amministrative indipendenti", Cedam, 2010

M. Clarich (2005-a), *Autorità indipendenti. Bilancio e prospettive di un modello*, il Mulino, 2005

M. Clarich (2005-b), *Le Autorità indipendenti: dopo l'ascesa il declino?*, in "il Mulino", 2005, n. 2

M. Clarich (2004), *Le autorità indipendenti nello "spazio regolatorio": l'ascesa e il declino del modello*, in "Diritto pubblico", 2004, n. 3

C. Colapietro (2022), *La proposta di Artificial Intelligence Act: quali prospettive per l'amministrazione digitale?*, in "CERIDAP", 2022, fasc. spec. n. 1

C. Colapietro (2021-a), *Circolazione dei dati, automatizzazione e regolazione*, in "Osservatorio sulle fonti", 2021, n. 2

C. Colapietro (2021-b), *Le sfide del "Costituzionalismo digitale": un approccio originale al rapporto tra diritto e nuove tecnologie*, in A. Lo Calzo, L. Pace, G. Serges et al. (a cura di), "Diritto e nuove tecnologie tra comparazione e interdisciplinarità", fasc. spec. monografico n. 3 della "Rivista del Gruppo di Pisa", 2021

C. Colapietro, A. Simoncini (2022), *Introduzione*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

E. Cremona (2021-a), *Fonti private e legittimazione democratica nell'età della tecnologia*, in "DPCE online", 2021, num. spec.

E. Cremona (2021-b), *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in "Osservatorio sulle fonti", 2021, n. 2

M. Cuniberti (2002), *Autorità amministrative indipendenti e Costituzione*, in "Rivista di Diritto Costituzionale", Giappichelli, 2002

M. D'Alberti (2009), *Le autorità di regolazione dei mercati: il valore dell'indipendenza*, in "Astrid Rassegna", 2009, n. 17

G. D'Ippolito (2020), *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in "Il Diritto dell'informazione e dell'informatica", 2020, n. 4

A. Davola (2021), *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in "Diritto di internet", 2021, n. 1

A. De Franceschi (2019), *Il «pagamento» mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

G. De Gregorio (2021), *The rise of digital constitutionalism in the European Union*, in "International Journal of Constitutional Law", vol. 19, 2021, n. 1

G. De Minico (2021), *Autorità indipendenti e algoritmi: una famiglia disfunzionale*, in "Osservatorio sulle fonti", 2021, n. 2

F. Donati (2017), *Democrazia pluralista e potestà normativa delle Autorità indipendenti*, in "Osservatorio sulle fonti", 2017, n. 3

F. Faini (2023), *Il dato personale tra protezione giuridica e valorizzazione economica*, in "Osservatorio sulle fonti", 2023, n. 2

F. Faini (2020), *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in "federalismi.it", 2020, n. 16

C. Faralli (2019), *Diritti e nuove tecnologie*, in "Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica", 2019, n. 2

L. Floridi (2017), *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017

C. Franchini (1996), *Le autorità indipendenti come figure organizzative nuove*, in S. Cassese, C. Franchini (a cura di), "I garanti delle regole", il Mulino, 1996

E. Frontoni (2024), *Governare le tecnologie e con le tecnologie: l'impatto sulla produzione normativa*, in "Osservatorio sulle fonti", 2024, n. 1

M. Giannelli (2021), *Poteri dell'AGCOM e uso degli algoritmi. Tra innovazioni tecnologiche ed evoluzioni del quadro regolamentare*, in "Osservatorio sulle fonti", 2021, n. 2

T. Groppi, A. Simoncini (2019), *Introduzione allo studio del diritto pubblico e delle sue fonti*, IV ed., Giappichelli, 2019

L. Gulino (2023), *Prospettive di tutela dei consumatori nel mondo digitale*, in G. Cerrina Feroni (a cura di), "Il ruolo del Garante per la protezione dei dati personali. La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro", il Mulino, 2023

A. Iannuzzi (2024-a), *I regolamenti intersettoriali per l'istituzione dei «data spaces»:* Data Governance Act *e* Data Act, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

A. Iannuzzi (2024-b), *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

A. Iannuzzi (2023), *Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione*, in "Bilancio Comunità Persona", 2023, n. 2

A. Iannuzzi (2021), *La* governance *europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

A. Iannuzzi (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018

S. Labriola (1999), *Le autorità indipendenti (note preliminari)*, in Id. (a cura di), "Le autorità indipendenti. Da fattori evolutivi ad elementi della transizione nel diritto pubblico italiano", Giuffrè, 1999

A. Lamberti (2022), *L'ambiente digitale: una sfida per il diritto costituzionale*, in "federalismi.it", 2022, n. 2

F. Laviola (2022), *Il diritto all'autodeterminazione informativa tra concorrenza e* data protection. *Riflessioni a margine della saga* Facebook c. Bundekartellamt *nella giurisprudenza delle corti tedesche e in attesa della Corte di Giustizia*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

F. Laviola (2021), *Diritti fondamentali ed efficienza economica nel mercato digitale: tra protezione dei dati personali e tutela della concorrenza*, in A. Lo Calzo, L. Pace, G. Serges et al. (a cura di), "Diritto e nuove tecnologie tra comparazione e interdisciplinarità", fasc. spec. monografico n. 3 della "Rivista del Gruppo di Pisa", 2021

F. Longo (1996), *Ragioni e modalità dell'istituzione delle autorità indipendenti*, in S. Cassese, C. Franchini (a cura di), "I garanti delle regole", il Mulino, 1996

N. Longobardi (2009), *Autorità amministrative indipendenti e sistema giuridico-istituzionale*, II ed., Giappichelli, 2009

C. Malinconico (1996), *Le funzioni amministrative delle autorità indipendenti*, in S. Cassese, C. Franchini (a cura di), "I garanti delle regole", il Mulino, 1996

M. Manetti (2007), *Le autorità indipendenti*, Laterza, 2007

M. Manetti (1999), *Le proposte di riforma costituzionale in materia di autorità indipendenti*, in Aa.Vv., "Autorità indipendenti e principi costituzionali. Atti del Convegno di Sorrento 30 maggio 1997", Cedam, 1999

A. Manganelli (2023), *Piattaforme digitali e social network, fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato*, in "Giurisprudenza costituzionale", 2023, n. 2

S. Mangiameli (2023), *La sovranità digitale*, in "dirittifondamentali.it", 2023, n. 3

P. Manzini (2023), *Antitrust e privacy: la strana coppia*, in "Quaderni AISDUE", 2023, n. 3

F. Merusi, M. Passaro (2003), *Le autorità indipendenti*, il Mulino, 2003

F. Mezzanotte (2018), *I poteri privati nell'odierno diritto dello sviluppo economico*, in "Politica del diritto", 2018, n. 3

M. Midiri (2021), *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in "Il Diritto dell'informazione e dell'informatica", 2021, n. 2

G. Mobilio (2024), *La co-regolazione delle nuove tecnologie, tra rischi e tutela dei diritti fondamentali*, in "Osservatorio sulle fonti", 2024, n. 1

G. Mobilio (2020), *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in "BioLaw Journal - Rivista di BioDiritto", 2020, n. 2

F. Modugno (2019), *Ordinamento, Diritto, Stato*, in Id. (a cura di), "Diritto pubblico", iv ed., Giappichelli, 2019

F. Modugno (1968), voce *Poteri (divisione dei)*, in "Novissimo Digesto Italiano", vol. xiii, UTET, 1968

S. Niccolai (1999), *Le autorità indipendenti nel progetto di revisione costituzionale*, in S. Labriola (a cura di), "Le autorità indipendenti. Da fattori evolutivi ad elementi della transizione nel diritto pubblico italiano", Giuffrè, 1999

M. Orofino (2024-a), *Il* Digital Market Act*: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

M. Orofino (2024-b), *Il* Digital Service Act *tra continuità (solo apparente) ed innovazione*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

C. Padovani, M. Santaniello (2018), *Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system*, in "International Communication Gazette", vol. 80, 2018, n. 4

V. Pagnanelli (2022), *Una "valutazione d'impatto" della privacy sulle big tech. Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

V. Pagnanelli (2021), *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in "Osservatorio sulle fonti", 2021, n. 2

R. Panetta (2024), *Governance dell'AI Act: il ruolo delle Autorità in Italia ed Europa*, in "Agenda Digitale", 21 giugno 2024

R. Pardolesi, R. Van Den Bergh, F. Weber (2020), *Facebook e i peccati da «Konditionenmissbrauch»*, in "Mercato concorrenza regole", 2020, n. 3

M. Passaro (1999), *Autorità o amministrazioni indipendenti? L'ambito semantico e l'identità concettuale*, in Aa.Vv., "Autorità indipendenti e principi costituzionali. Atti del Convegno di Sorrento 30 maggio 1997", Cedam, 1999

M. Pietrangelo (2023), *Spazio digitale e modelli di regolazione*, in "Consulta online", 2023, n. 3

G. Pistorio (2024), *La co-regolazione nell'ecosistema digitale tra etero-regolazione e auto-regolazione. Questioni definitorie*, in "Osservatorio sulle fonti", 2024, n. 1

G. Pitruzzella (2024), *La tutela della concorrenza nella recente giurisprudenza della Corte di Giustizia*, in "federalismi.it", 2024, n. 9

G. Pitruzzella (2023), *Le Autorità amministrative indipendenti: bilancio e prospettive*, in G. Cerrina Feroni, "Il ruolo del Garante per la protezione dei dati personali: la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro", il Mulino, 2023

F. Pizzetti (2024), *Introduzione alla regolazione europea della società digitale*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

O. Pollicino (2022), *I codici di condotta tra* self-regulation *e* hard-regulation*: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione* online, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

O. Pollicino (2021), *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali le sfide per il giurista (teorico e pratico)?*, in "Giustizia insieme", 15 aprile 2021

O. Pollicino (2019), *New Technology, Algorithms and the Rising of Private (Digital) Powers and new Challenges for Constitutional Law*, in "EUreka!", 11 July 2019

O. Pollicino, G. De Gregorio (2021), *Constitutional Law in the Algorithmic Society*, in H.-W. Micklitz, O. Pollicino, A. Reichman et al., "Constitutional Challenges in the Algorithmic Society", Cambridge University Press, 2021

A. Predieri (1997), *L'erompere delle autorità amministrative indipendenti*, Passigli Editori, 1997

M. Rabitti (2020), *Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento*, RomaTrE-Press, 2020

G. Resta (2019), *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, n. 2

V. Ricciuto (2019), *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

A. Riviezzo (2005), *Autorità amministrative indipendenti e ordinamento costituzionale*, in "Quaderni costituzionali", 2005, n. 2

M. Ruotolo (2020), *Corso di diritto costituzionale. Fonti, diritti, giustizia costituzionale*, Giappichelli, 2020

M. Savino (2001), *L'indagine conoscitiva del Parlamento*, in F.A. Grassini (a cura di), "L'indipendenza delle autorità", il Mulino, 2001

G. Scorza (2022), *In principio era Internet e lo immaginavamo diverso*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Simoncini (2022), *La co-regolazione delle piattaforme digitali*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di Stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2

A. Simoncini, E. Cremona (2021), *La AI fra pubblico e privato*, in "DPCE online", 2021, n. 1

C. Storace (2024), *La digitalizzazione della giustizia: spunti di riflessione per un modello di co-regolazione costituzionalmente orientato*, in "Osservatorio sulle fonti", 2024, n. 1

G. Tarli Barbieri (2021), *Considerazioni di sintesi sul ruolo delle autorità amministrative indipendenti nella regolazione delle decisioni algoritmiche*, in "Osservatorio sulle fonti", 2021, n. 2

R. Titomanlio (2017), *Riflessioni sul potere normativo delle Autorità amministrative indipendenti fra legalità "sostanziale", legalità "procedurale" e funzione di regolazione*, in "Nomos", 2017, n. 1

L. Torchia (2022), *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

R. Van den Bergh, F. Weber (2021), *The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law?*, in "World Competition", vol. 44, 2021, n. 1

F. Zammartino (2020), *Il modello molteplice. La potestà normativa delle Autorità amministrative indipendenti*, Giappichelli, 2020

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, trad. it. P. Bassotti, Luiss University Press, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0217 • articolo sottoposto a peer review • pubblicato in anteprima il 7 mag. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Antonio Cremone

Libertà di espressione e nuove tecnologie: *a complicated relationship*

Il contributo esplora il ruolo delle piattaforme digitali nella diffusione del pensiero, analizzando la complessità giuridica e sociale che emerge nella regolamentazione dei contenuti online, tenendo conto che la diffusione di Internet e delle piattaforme social ha ampliato l'accesso alla comunicazione (consentendo a chiunque di esprimere le proprie idee), ma richiede anche la capacità di fronteggiare nuove sfide, passibili di minacciare il dibattito democratico. Nel dettaglio, vengono affrontati temi quali fake news, hate speech e l'interazione tra giurisdizioni nazionali e politiche aziendali private, esaminando l'evoluzione delle tecniche di regolazione, passate dalle politiche di soft law al Digital Services Act (DSA) approvato dall'Unione europea, nell'ambito di una più ampia strategia volta a creare un ambiente digitale più sicuro e trasparente. Attraverso l'esame di casi pratici, poi, si riflette sulle sfide poste dalle piattaforme, vagliando l'estensione ad esse di ipotesi di responsabilità simil-editoriale. Infine, nel delineare i possibili equilibri tra libertà di espressione e responsabilità, si conclude con una riflessione sul "sesto potere" esercitato dalle piattaforme nelle zone grigie del diritto, e sul suo impatto sulle dinamiche pubbliche.

Digitalizzazione – Notizie false – Discorsi d'odio – Piattaforme – Responsabilità

Freedom of expression and new technologies: a complicated relationship

This article explores the role of digital platforms in the dissemination of thought, analyzing the legal and social complexities that arise in the regulation of online content. It highlights that the rise of the internet and social platforms has expanded access to communication (allowing anyone to express their ideas) but also requires the ability to face new challenges that could threaten democratic debate. Specifically, issues such as fake news, hate speech, and the interaction between national jurisdictions and private corporate policies are addressed, examining the evolution of regulatory techniques, from soft law policies to the EU Digital Services Act (DSA), as part of a broader European strategy to create a safer and more transparent digital environment. Through the analysis of practical cases, the text reflects on the challenges posed by platforms, considering the extension of editorial-like liability to them. Finally, in outlining the possible balance between freedom of expression and liability, it concludes with a reflection on the "sixth power" exercised by platforms in the grey areas of the law and its impact on public dynamics.

Digitalization – Fake news – Hate speech – Platforms – Liability

L'Autore è assegnista di ricerca 2023-24 presso l'Università degli Studi di Firenze

Sommario: 1. Digitalizzazione e manifestazione del pensiero. – 2. Fake news, hate speech, giurisdizioni e *private policies*. – 3. Oltre le *private policies*: dal *soft law* al DSA. – 4. Cenni a (e riflessioni su) alcuni casi pratici. – 5. Considerazioni *in itinere*. – 5.1. Una prima riflessione sulle piattaforme. – 5.2. Note sulla possibile previsione di una responsabilità simil-editoriale: dai casi Uber e Airbnb alla valorizzazione dell'hosting attivo. – 5.3. Un passo indietro: dai pensieri ai contenuti. – 6. Sesto potere e sovranità nelle "zone grigie".

1. Digitalizzazione e manifestazione del pensiero

Questo contributo, inserendosi in un più ampio percorso di ricerca sui nuovi scenari della digitalizzazione[1], intende affrontare alcuni recenti accadimenti e provvedimenti che riflettono i propri effetti sulla libertà di espressione, ossia sul diritto (di tutti[2]) di manifestare il proprio pensiero[3] verso un pubblico ampio e indeterminato di persone, in forma orale o scritta, attraverso ogni possibile mezzo di comunicazione[4].

In merito a tale diritto, che costituisce una delle principali prerogative di uno Stato che possa definirsi effettivamente democratico[5], nell'ordinamento italiano si è assistito ad una progressiva estensione del portato dell'art. 21 Cost., al punto da

1. Assegno di ricerca presso l'Università degli studi di Firenze, avente ad oggetto la "Realizzazione iniziative comuni nell'ambito dello sviluppo del Centro di competenza 5G e tecnologie innovative", nell'ambito dei seguenti programmi di ricerca: Progetto "Fondi Progetto PRIN 2017: Self- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law (SE.CO.R.ETEC)" responsabile Andrea Simoncini; Progetto "Fondi Accordo di ricerca Regione Toscana rep.2023/2955" responsabile Andrea Simoncini, progetto 23SIMONCINI5G.
2. Non solo dei professionisti dell'informazione o dei cittadini di uno Stato, ma anche di chi ivi – per qualsivoglia ragione – si trovi.
3. Attenendosi più strettamente al disposto dell'art. 21 co. 1 Cost., secondo cui "Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione".
4. Groppi–Simoncini 2012, p. 133.
5. Martines 2000, p. 551, secondo cui "appare evidente… che un regime in cui non sia possibile manifestare liberamente il proprio pensiero non può certamente definirsi democratico ma anche che la 'democraticità' di un ordinamento è direttamente proporzionale al grado in cui la libera manifestazione del pensiero viene riconosciuta ed in concreto attuata". Non a caso, l'art. 21 Cost. prevede, per il sequestro della stampa una riserva di legge e di giurisdizione, condizioni anche più stringenti rispetto alle restrizioni alla libertà personale (si pensi ai dimezzati termini di cui all'art. 21 co. 4 Cost.). Nel medesimo solco si pongono C. cost. 17 aprile 1969, in *Giur. it.*, 1969, I, p. 1854, secondo cui la libertà di propaganda, in quanto manifestazione della libertà d'espressione "trova collocazione tra i cardini essenziali dell'ordine democratico", nonché C. cost. 8 luglio 1971, n. 168, in *Giur. cost.*, 1971, I, p. 1780, che inserisce il diritto in parola tra "diritti primari e fondamentali (come il più alto, forse…)". L'imprescindibilità di tale diritto emerge anche dall'art. 11 della Dichiarazione francese dei diritti dell'uomo del 1789, secondo cui "La libera manifestazione dei pensieri e delle opinioni è uno dei diritti più preziosi dell'uomo; ogni cittadino può dunque parlare, scrivere, stampare liberamente, salvo a rispondere dell'abuso di questa libertà nei casi determinati dalla Legge".

ricollegarvi la libertà di informazione[6], il diritto di cronaca[7], ma anche la diffusione di pensieri altrui (salvo il diritto d'autore[8]) e di notizie di attualità, nel rispetto dei limiti espliciti[9] e/o impliciti[10] previsti dall'ordinamento.

Dando per nota la disciplina prevista per la stampa[11] e la radiotelevisione[12] (i mezzi di diffusione del pensiero – almeno in origine – più diffusi[13]), va osservato come alcune criticità sollevate in merito alle concrete possibilità di accesso a tali strumenti[14] e (quindi) all'effettiva implementazione di un modello pluralistico[15], siano state superate dal dirompente impatto delle nuove tecnologie che, attraverso la diffusione di Internet (prima) e delle

6. Intesa come libertà di informare e di essere informati, attraverso una pluralità di strumenti e fonti di informazione (c.d. pluralismo), in conformità agli artt. 21, 41 e 3 Cost.
7. Inteso, a livello individuale, come la libertà del singolo giornalista di interpretare la realtà, così svolgendo un ruolo di intermediazione tra i fatti e la loro diffusione, che consente anche manifestazioni non imparziali, sempreché non distorte, nel rispetto delle regole – anche deontologiche – alle quali sono sottoposti gli operatori dell'informazione professionale, che impongono un serio e diligente lavoro di ricerca dei fatti esposti.
8. Per gli scritti protetti.
9. Il buon costume, *in primis*, espressamente citato dall'art. 21 co. 6 Cost. (secondo cui "sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume"), inteso secondo l'opinione prevalente quale comune senso del pudore e pubblica decenza, anche (ma non solo) a tutela dei minori (cfr. Papa 2021-a, p. 68 ss.).
10. Correlati agli interessi costituzionalmente protetti (*in primis*, ma non solo, dagli artt. 2, 3, 14, 15 e 17 Cost.), quali la dignità, l'onore, la reputazione, l'identità personale, la riservatezza, il buon andamento della giustizia, la sicurezza dello Stato, il rispetto delle istituzioni e delle religioni, l'ordine pubblico, il diritto d'autore e le opere d'ingegno, ecc. (cfr. Papa 2021-a, p. 70 ss.; analogamente Borrello 2023, p. 36 ss.).
11. Che ricomprende, secondo l'art. 1 della legge 8 febbraio 1948 n. 47 "tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici in qualsiasi modo destinate alla pubblicazione". Sulla disciplina dell'editoria, di recente: Flore 2023, p. 235 ss.; Napolitano 2021, p. 79 ss.; Caretti–Cardone 2019, p. 33 ss.
12. Definito "un servizio sociale, in quanto diretto ad assicurare, agevolando la circolazione delle idee, l'effettività della libera manifestazione del pensiero e della libertà di informazione, considerate come due aspetti essenziali ed inscindibili di un unico valore costituzionalmente protetto in via primaria dell'art. 21 Cost." (C. cost. 25 maggio 1987, n. 194, in *Giur. it.*, 1988, I, 1, p. 329). Sulla disciplina della radiotelevisione, di recente: Musselli 2023, p. 265 ss.; Giglioni 2023, p. 289 ss.; Messina 2021, p. 109 ss.; Caretti–Cardone 2019, p. 103 ss.
13. Senza comunque dimenticare, ovviamente, il ruolo degli spettacoli cinematografici e teatrali, per la cui disciplina si rinvia a Caretti–Cardone 2019, p. 271 ss.
14. Cfr. C. cost. 15 giugno 1972, n. 105, in CED Cassazione 1972, secondo cui "che 'tutti' abbiano diritto di manifestare il proprio pensiero 'con ogni mezzo', non può significare che tutti debbano avere, in fatto, la materiale disponibilità di tutti i possibili mezzi di diffusione, ma vuol dire, più realisticamente, che a tutti la legge deve garantire la giuridica possibilità di usarne o di accedervi, con le modalità ed entro i limiti resi eventualmente necessari dalle peculiari caratteristiche dei singoli mezzi o dalla esigenza di assicurare l'armonica coesistenza del pari diritto di ciascuno o dalla tutela di altri interessi costituzionalmente apprezzabili, giusta i criteri di cui questa Corte ha fatto applicazione in varie occasioni (sentenze n. 59 del 1960, n. 48 del 1964, n. 11 del 1968)".
15. Si pensi, a titolo esemplificativo, allo strumento radiotelevisivo, originariamente in mano pubblica (seppur mitigato dal c.d. pluralismo interno, relativo ai contenuti trasmessi), poi caratterizzato da un duopolio di fatto (in parte correlato alla limitata disponibilità di frequenze), che ha raggiunto solo di recente, e all'esito di alterne e variegate vicende (anche giudiziali), una conformazione effettivamente "aperta" (c.d. pluralismo esterno, correlato anche alla libertà di concorrenza), rispetto ad un modello pubblico-privato in precedenza oligopolistico (sul tema, C. cost. 14 luglio 1988, n. 826, in *Giur. cost.*, 1988, I, p. 3893, secondo cui "Il servizio pubblico televisivo deve favorire l'espressione di tutte o del maggior numero possibile delle correnti di opinione esistenti della comunità; le libertà assicurate alle imprese radiotelevisive limita il pluralismo (c.d. interno). La pluralità

piattaforme social e media (poi), hanno consentito a chiunque (o quasi[16]) di poter accedere a nuove opportunità di comunicazione ed esercitare attraverso di esse (con enorme facilità/rapidità e senza particolari costi, seppur con i limiti che vedremo) la propria libertà di espressione[17].

Tale cambiamento, consentendo la condivisione in tempo reale di contenuti di ogni tipo, e la (altrettanto rapida) propagazione degli stessi nei confronti di un numero potenzialmente indeterminato di destinatari, se da un lato ha rivoluzionato favorevolmente le modalità di esercizio del diritto *de quo* (rimuovendo i principali suoi ostacoli: le barriere economiche alla diffusione del pensiero attraverso gli strumenti tradizionali[18], ma anche la necessaria "intermediazione" delle informazioni da parte di soggetti specializzati[19]), dall'altro ha determinato (o agevolato) l'insorgenza di ulteriori criticità, spesso identificate con terminologia anglofona (fake news, deep fake, hate speech, cyberbullismo, cyberstalking, revenge porn, ecc.), sulle quali pare opportuno articolare delle riflessioni.

Riflessioni che si soffermeranno (anche alla luce dell'adozione di alcuni recenti – e rilevanti – provvedimenti eurounitari) su specifiche tipologie di contenuti anomali e/o illegali[20] (fake news e hate speech), poiché caratterizzati da una maggiore propensione a turbare il corretto svolgersi del dibattito pubblico (anche in termini di diritto all'informazione), implementando un clima di post-verità[21] e un rischio di riduzione della partecipazione al dibattito pubblico[22], che mette a dura prova il corretto funzionamento dei meccanismi democratici[23].

E ciò, ovviamente, senza la pretesa (o la presunzione) di poter fornire agevoli soluzioni, nella

d'informazione non è garantita dalla coesistenza del servizio pubblico radiotelevisivo e da un polo privato, con posizione dominante nel settore privato".

16. Il "quasi" è d'obbligo, in considerazione dei limiti oggettivi (esistono aree, in Europa e nel nostro Paese, non adeguatamente raggiunte da Internet) e soggettivi (si pensi al digital divide, espressione nata in seno all'amministrazione statunitense della presidenza Clinton 1993-2001 per indicare la disparità nelle possibilità di accesso ai servizi telematici tra la popolazione americana, ed oggi diffusa a livello mondiale, quale consapevolezza di una problematica di accesso ai mezzi di informazione e comunicazione da parte di determinate aree geografiche o fasce di popolazione – così Granelli 2008), che ancora impediscono una piena fruizione dei servizi e delle opportunità digitali.
17. Cfr. Pollicino 2018, p. 4 ss., che traccia anche l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo in tema di libertà d'espressione.
18. In tal senso si segnala Pitruzzella 2018, che evidenzia come – prima dell'avvento degli strumenti di comunicazione digitali – la diffusione di contenuti richiedesse ingenti investimenti "indispensabili per organizzare gli stabilimenti tipografici e le redazioni con cui si producevano i giornali, per realizzare il telegrafo e la rete telefonica, le radio e le televisioni, la tv via cavo e la tv satellitare".
19. Anche in considerazione della natura non illimitata dei canali di diffusione delle comunicazioni (canali tv, frequenze radio, ecc.).
20. Classificati talvolta in modo confuso dalle stesse piattaforme ospitanti, che sovrappongono *inappropriate content*, *sensitive content*, *objectionable content*, *illegal content*, *prohibited content*, *violative content*, ecc. (si veda, in tal senso, il contributo di Combei 2023).
21. Si segnala, a tal riguardo, la stretta correlazione tra "fake news" e "post-truth", termine definito dall'Oxford Dictionary come "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief".
22. Cfr. Tanzarella 2023, p. 153, che rimarca come la diffusione dei discorsi di odio porti le vittime ad assumere un atteggiamento remissivo, astenendosi dal dibattito democratico e pregiudicando il pluralismo di idee che la libertà di manifestazione del pensiero dovrebbe invece presidiare.
23. Si pensi, *inter alia*, a quanto accaduto per la Brexit del 2016, le elezioni americane del 2016 e del 2020, le consultazioni elettorali e referendarie italiane del 2016, del 2018 e del 2022, per i quali si segnalano: Mezzanotte 2018, p. 18; Molinari 2019, p. 114 ss.; Di Gregorio 2019, p. 7 ss.; Palici di Suni 2020, p. 140 ss., Candido 2020, p. 105 ss.; Galeotti 2021, p. 64 ss.; Pollicino–Dunn 2024, p. 4 ss.

consapevolezza che l'analisi di fenomeni giuridico-sociali complessi, tanto più se (anche fisiologicamente[24]) *in itinere*, ponga spesso più interrogativi che risposte, e che – come in ogni *complicated relationship* (da cui il titolo) – sia necessario abbandonare preconcetti e soluzioni radicali, in favore di valutazioni ponderate ed equi bilanciamenti.

2. Fake news, hate speech, giurisdizioni e *private policies*

La prima criticità sulla quale pare opportuno soffermarsi è quella delle c.d. fake news, ossia di "notizie false, con particolare riferimento a quelle diffuse mediante la Rete"[25]. Non, quindi, la semplice disinformazione (diffusa *ad hoc* oppure in buona fede[26]), ma quella propagata attraverso Internet, in modo più o meno consapevole[27].

Il fenomeno, in linea di massima, rientra tra le manifestazioni della libertà d'espressione, la quale – secondo l'opinione prevalente – non richiede che il pensiero diffuso sia necessariamente utile alla comunità[28], ritenendolo legittimo anche se falso, a patto che non siano lesi i diritti fondamentali e non venga pregiudicato l'ordine pubblico[29].

Tale condotta è infatti passibile di responsabilità penale, ai sensi dell'art. 595 c.p.[30] (ove si leda l'altrui reputazione), ovvero dell'art. 656 c.p.[31] (allorquando le notizie false diffuse siano idonee a turbare

24. In considerazione della velocità dei cambiamenti tecnologici, che costringe il diritto allo scomodo ruolo di inseguitore.
25. Cfr. Vocabolario online neologismi Treccani, 2017.
26. Distingue le fake news in tali due macrocategorie Monti 2022, p. 195.
27. Non a caso, l'Oxford Dictionary definisce le fake news come "news that conveys or incorporates false, fabricated, or deliberately misleading information, or that is characterized as or accused of doing so", ricomprendendo anche (ma non solo) le notizie false diffuse in modo deliberato. Va comunque segnalata l'opinione secondo cui per fake news dovrebbero intendersi solo quelle diffuse in modo consapevole, come rimarcato da Marchetti 2023, p. 462.
28. Cfr. Papa 2021, p. 61, secondo cui "ne deriva che il pensiero espresso possa anche essere frutto di fantasia, o essere non veritiero, a condizione che non consista nella pubblicazione e diffusione di notizie false, esagerate o tendenziose, per le quali possa essere turbato l'ordine pubblico. In presenza di questa ipotesi, trova applicazione infatti l'art. 656 c.p., anche se spetta inevitabilmente al Giudice la valutazione della reale idoneità della notizia diffusa a configurare un pericolo per la pacifica e regolare convivenza dei consociati".
29. In tal senso, si legga anche Marchetti 2023, p. 466 ss., ove si rimarca (con richiami di giurisprudenza) che "la nostra Costituzione non tutela espressamente il diritto a ricevere informazioni veritiere e nemmeno dalla giurisprudenza costituzionale sembra emergere che la libertà di essere informati comporti un diritto a essere informati in maniera corretta […] essendo sufficiente garantire la rimozione degli ostacoli che possono impedire la circolazione e la ricezione delle informazioni", e che anche per i giornalisti "la verità della notizia […] assume […] rilevanza solo ai fini di attribuire la responsabilità al soggetto che l'ha pubblicata, ledendo interessi altrui, non per ostacolarne la diffusione". Nel medesimo senso, si legga anche la Comunicazione congiunta del 2020 della Commissione Ue e dell'Alto rappresentante intitolata "Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti" – JOIN(2020) 8, che ritiene legittimi i contenuti falsi, ma diffusi senza intenzioni fraudolente, qualificandoli come "contenuti dannosi ma non illegali".
30. Secondo cui "Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate".
31. Secondo cui "Chiunque pubblica o diffonde notizie false, esagerate o tendenziose, per le quali possa essere turbato l'ordine pubblico, è punito, se il fatto non costituisce un più grave reato, con l'arresto fino a tre mesi o con l'ammenda fino a euro 309".

l'ordine pubblico), ma si rivela assai pericolosa anche al di fuori delle ipotesi di reato. Non può trascurarsi, del resto, come la predetta dinamica – anche attraverso i meccanismi della profilazione e della correlata personalizzazione dei contenuti proposti all'utente (c.d. "filter bubble"[32]) – tenda a polarizzare il dibattito (c.d. "group polarization"[33]), irrigidendo le posizioni e determinando fenomeni discriminatori nei confronti di chi rappresenti punti di vista differenti rispetto a quelli che aggregano determinati gruppi di soggetti, in tal modo condizionando l'opinione pubblica al di fuori dei circuiti di tutela previsti dalla Costituzione[34].

La seconda criticità è quella del c.d. hate speech, ossia della "espressione di odio rivolta, in presenza o tramite mezzi di comunicazione, contro individui o intere fasce di popolazione (stranieri e immigrati, donne, persone di colore, omosessuali, credenti di altre religioni, disabili, ecc.)"[35].

Trattasi di una condotta "ai confini estremi della libertà di manifestazione del pensiero"[36], a sua volta passibile di responsabilità penale, ai sensi dell'art. 604-*bis* c.p.[37] (ma anche di responsabilità civile[38]), allorquando vi sia propaganda e istigazione a delinquere per motivi di discriminazione razziale[39], etnica e religiosa.

32. Definito dall'enciclopedia Treccani, Neologismi, 2017, come "l'ambiente virtuale che ciascun utente costruisce in internet tramite le sue selezioni preferenziali, caratterizzato da scarsa permeabilità alla novità e alto livello di autoreferenzialità".
33. Intesa, nelle scienze psicologiche, come la tendenza degli individui membri di un gruppo ad assumere sistematicamente e in modo graduale delle posizioni più estreme rispetto alla media delle posizioni iniziali dei restanti membri (definizione rinvenuta in Colman 2015).
34. Fondati, come noto, sulla correttezza e sul pluralismo dell'informazione.
35. Cfr. Vocabolario online neologismi Treccani, 2018.
36. Tanzarella 2023, p. 151, che evidenzia come l'interrogativo da porsi sia quello di stabilire se le parole debbano o meno essere trattate al pari degli atti concreti.
37. Secondo cui "Salvo che il fatto costituisca più grave reato, è punito: a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi; b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi. È vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni. Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale". Il contenuto di tale norma è riconducibile all'art. 3 della legge 13 ottobre 1975, n. 654, come modificato nel 1993 e nel 2006, trasposto nel codice penale con il d.lgs. 1° marzo 2018, n. 21.
38. Nei termini di cui agli artt. 4 ss. del d.lgs. 9 luglio 2003, n. 215 (che attua la direttiva comunitaria 2000/43/CE), ma anche secondo quanto previsto per le telecomunicazioni dalla legge c.d. Gasparri 3 maggio 2004, n. 112, che vieta la trasmissione di programmi "che contengono incitamenti all'odio" (sui rimedi civilistici, si rinvia all'analisi di Tanzarella 2023, p. 157 ss.).
39. Discriminazione razziale intesa dalle corti supreme europee in senso c.d. differenzialista, come evidenziato da Monti 2022, p. 194 ss., il quale evidenzia tuttavia come una applicazione estensiva delle disposizioni anti hate-speech, secondo tale nuovo concetto di razzismo, rischi di punire e criminalizzare condotte espressive che critichino certe visioni della società multiculturale; sui medesimi temi, si segnala anche Scaffardi 2009, p. 230.

La terza criticità, invece, riguarda il peculiare approccio che, rispetto all'inquadramento giuridico di tali fenomeni, deriva dai diversi confini della libertà di espressione negli ordinamenti Ue e USA, la cui disamina[40] si rivela utile, ove si considerino alcune semplici circostanze: 1) dagli Stati Uniti provengono quasi tutti gli attori digitali (motori di ricerca, canali di diffusione video e social network) attraverso cui vengono diffusi i contenuti in ambito europeo; 2) il Primo emendamento alla Costituzione USA[41] promuove un'interpretazione della libertà di espressione particolarmente estesa (e non esente da critiche[42]), al punto da vietare finanche al Congresso di promulgare leggi che la limitino, mentre in Ue l'approccio è maggiormente cauto, essendo ammessi – come anche per il nostro ordinamento nazionale – limiti espliciti ed impliciti; 3) con specifico riferimento ai discorsi d'odio, poi, si pone anche il problema della differente valutazione di pericolosità tra ordinamento europeo e statunitense, ove il primo tende a censurare i discorsi di odio in sé (per la propria astratta capacità di incidere sulle dinamiche democratiche)[43], mentre il secondo tende a valorizzare la pericolosità in concreto (intesa come effettiva e concreta incidenza sul possibile aumento di attività illecite)[44]; 4) soluzioni di moderazione dei contenuti "territorializzate"[45], per quanto astrattamente realizzabili, sarebbero antieconomiche e disfunzionali[46], presupporrebbero un controllo dei contenuti e

40. Puntualmente effettuata da Monti 2022, p. 197 ss.
41. Testualmente "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances" (tradotto: "Il Congresso non promulgherà leggi per il riconoscimento ufficiale di una religione, o che ne proibiscano la libera professione; o che limitino la libertà di parola, o della stampa; o il diritto delle persone di riunirsi pacificamente in assemblea e di fare petizioni al governo per la riparazione dei torti").
42. Saunders 1996.
43. Risultando tutelato, quale bene della vita, il rispetto della dignità umana, in chiave individuale, rilevato che la condotta censurata colpisce prima l'individuo e poi la comunità, a dispetto della pericolosità in concreto, che tende a tutelare l'ordine pubblico. In tal senso, senza pretesa di esaustività, si segnalano in ambito sovra e infra-nazionale: la recente pronuncia della CGUE, Grande Sezione, 23 aprile 2020 n. 507, in *Foro it.*, 2020, 6, IV, p. 293, che ha sanzionato un avvocato italiano per aver dichiarato che non avrebbe assunto persone omosessuali nel proprio studio, pur in assenza – al momento della dichiarazione – di una concreta procedura di reclutamento; la sentenza CEDU 15615/2007 del 16 luglio 2009, *Feret c. Belgio*, in *Cass. pen.*, 2010, 2, p. 852, secondo cui "Attacchi che si concretizzano in insulti, la messa in ridicolo o la calunnia ai danni di specifici gruppi di una popolazione sono motivi sufficienti per le autorità per combattere l'hate speech, sfavorendo così la libertà d'espressione esercitata in maniera irresponsabile"; Cass. pen., sez. III, 13 dicembre 2007 n. 13234, in *CED Cassazione penale* 2008, secondo cui "l'oggetto specifico della tutela penale […] non è costituito dall'ordine pubblico, il quale ha una rilevanza indiretta, ma dalla tutela della dignità umana"; Cass. pen., sez. I, 22 novembre 2012 n. 47894, in *Guida al diritto*, 2013, 4, p. 49, ove si afferma che "l'elemento che caratterizza la fattispecie è la propaganda discriminatoria, intesa come diffusione di un'idea di avversione argomentata sulla ritenuta diversità e inferiorità, senza che tale condotta debba necessariamente caratterizzarsi per la capacità di condizionare o influenzare il comportamento di un vasto pubblico in modo da raccogliere adesioni".
44. Per una attenta disamina di tali aspetti, cfr. Monti 2022, p. 200 ss., che evidenzia (quali eccezioni alle tendenze indicate) la propensione della Corte costituzionale italiana alla valutazione di pericolosità in concreto, e quella dell'ordinamento statunitense alla valutazione di pericolosità in astratto per i discorsi d'odio correlati al terrorismo jhiadista.
45. C.d. *geo-blocking*.
46. Sul tema, emblematico è il comunicato stampa del Parlamento europeo del 13 dicembre 2023 *Geoblocking: rivedere regole UE per eliminare tutte le limitazioni geografiche*, secondo cui le norme UE in materia di blocchi geografici devono essere applicate meglio e aggiornate per rafforzare il mercato unico digitale e rispondere meglio alle aspettative dei consumatori.

della loro diffusione di regola non previsto (come si chiarirà meglio nella "quarta criticità" affrontata), oltre che una capacità di verifica così capillare da non poter essere riservata all'attività umana, ma solo ad algoritmi (con implicazioni, anche etiche e di conformità alle disposizioni in tema di privacy, assai problematiche), anche per tentare di individuare l'originario autore/divulgatore del contenuto censurato, in un contesto (la rete) che agevola l'anonimato[47].

La quarta criticità, come anticipato, riguarda l'assenza di una c.d. responsabilità editoriale[48] in capo alle piattaforme (e, in generale, ai siti informativi non registrati come testate giornalistiche[49]), che determina l'assenza dei tradizionali controlli sui contenuti previsti per la stampa e la radiotelevisione, lasciando agli operatori del settore maggiori spazi di libertà nell'attività di moderazione, prevista negli USA dalla sez. 230[50] del CDA del 1996 e nell'Ue (in origine, prima dell'approvazione del

47. Si segnalano, a tal riguardo, i seguenti interessanti contributi: Cipolloni 2023, p. 518 ss., che considera l'anonimato anche quale limite alla protezione dei diritti della personalità; Betzu 2022, p. 392 ss.; Di Corinto 2022, p. 31 ss., che esamina proprio il rapporto tra anonimato e disinformazione; Di Tano–Brighi 2019, p. 183 ss., che evidenzia come l'anonimato agevoli crimini di odio, molestie e violenze; Manetti 2014, p. 139 ss., che evidenzia come l'anonimato sia invece giustificato e utile per garantire il diritto di informazione, senza esporre i soggetti interessati al rischio di ritorsioni; Vigevani 2014, p. 207 ss., che esamina il rapporto tra anonimato, trasparenza e partecipazione alla vita pubblica; Betzu 2011, che evidenzia il rischio di un potere senza responsabilità; Di Ciommo 2003, p. 117 ss., che già tempo addietro rimarcava l'esigenza di sottrarre Internet al cono d'ombra della deregolamentazione; Riccio 2000, p. 314 ss., secondo cui gli Internet provider devono accertare la reale identità dei fruitori del servizio.

48. Che, secondo la legislazione nazionale, ricade sia civilmente che penalmente sul direttore e/o sul vicedirettore responsabile (cfr. artt. 3 e 11 l. 8 febbraio 1948, n. 47, recante "Disposizioni sulla stampa", nonché art. 57 c.p.), in quanto responsabili di tutto ciò che viene pubblicato sulla testata, nonché – in solido con gli autori del reato, ma solo civilmente – sul proprietario della pubblicazione e sull'editore (*ex* art. 11 legge citata, ma anche ai sensi dell'art. 2049 c.c.). Per i profili generali, si rinvia a Cuniberti 2022, p. 283 ss. Sul tema si segnala, in merito alla possibile estensione della responsabilità editoriale anche alle testate giornalistiche telematiche, il lavoro di Lucchi 2011, p. 415 ss., nonché il successivo *revirement* di Cass. pen., sez. V, 11 dicembre 2017, n. 13398, commentato da Vimercati 2018, p. 324.

49. Cfr. Cass. pen., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 2018, 11, p. 3743 (con nota di Pedullà 2018), che, richiamando la sentenza Cass. SS.UU. 29 gennaio 2015, n. 31022, in *Giur. cost.*, 2015, 3, p. 1055 (con nota di Diotallevi 2015), ha affermato che solo le testate giornalistiche telematiche soggiacciono alla disciplina costituzionale e ordinaria prevista per la stampa, con inapplicabilità dell'art. 57 c.p.; in senso analogo Cass. pen. Sez. V, 8 novembre 2018, n. 12546, in *Ilpenalista.it*, 13 maggio 2019 (con nota di Sellaroli 2019).

50. In conformità alla sezione 230 del *Communication Decency Act* (CDA) del 1996, secondo cui "(1) Treatment of publisher or speaker – No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability – No provider or user of an interactive computer service shall be held liable on account of: (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)"; in italiano: "(1) Trattamento dell'editore o dell'autore – Nessun fornitore o utente di un servizio informatico interattivo sarà considerato l'editore o l'autore di qualsiasi informazione fornita da un altro fornitore di contenuti informativi. (2) Responsabilità civile – Nessun fornitore o utente di un servizio informatico interattivo potrà essere ritenuto responsabile a causa di: (A) qualsiasi azione volontariamente intrapresa in buona fede per limitare l'accesso o la disponibilità di materiale che il fornitore o l'utente considera osceno, lascivo, lussurioso, volgare, eccessivamente violento, molesto o altrimenti discutibile, che tale materiale sia o meno protetto costituzionalmente; o (B) qualsiasi azione intrapresa per consentire o mettere a disposizione ai fornitori di contenuti informativi o

Digital Service Act nel 2022) dagli artt. 13 e 14 della Direttiva sul commercio elettronico del 2000[51] (con imposizione ai fornitori di servizi di rimuovere i contenuti illeciti, ma solo su segnalazione e senza obbligo autonomo di iniziativa/monitoraggio[52]).

La quinta criticità è costituita proprio dall'attività di moderazione dei contenuti, disciplinata (e "giustiziata"[53]) in origine dalle stesse piattaforme, che hanno acquisito nel tempo un potere economico tale da tradursi (anche grazie alla profilazione[54] – non sempre legittima[55] – degli utenti) in un'influenza politico-sociale debordante, e che hanno imposto *policy* contrattuali[56] predisposte in regime di oligopolio[57], la cui applicazione ha suscitato non pochi dibattiti[58]. Dibattiti correlati anche al fatto che le *policy* di moderazione sono ricondotte, in ambito europeo, ad una dimensione meramente contrattual-privatistica (conseguente all'assenza di una adeguata disciplina pubblica) mentre, in ambito statunitense[59], vengono ricollegate ad una

ad altri i mezzi tecnici per limitare l'accesso al materiale descritto nel paragrafo (1)". Per la ricostruzione della normativa statunitense antecedente, si rinvia a Bassini 2019, p. 127 ss.

51. Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, recepita in Italia con d.lgs. 9 aprile 2003, n. 70.
52. Cfr. articolo 13 – *Memorizzazione temporanea detta "caching"* e articolo 14 – *Hosting*.
53. Il pensiero va agli organi di giustizia interna delle piattaforme, volti all'applicazione delle policy di ciascuna community, tra i quali spicca l'*Independent Oversight Board* di Facebook. Sul tema si rinvia a: Ruffolo 2024, p. 442 ss.; Asprella 2023, p. 241 ss., che nega la natura giurisdizionale dell'IOB di Facebook; Bucalo 2023, p. 143 ss., che evidenzia la natura para-giurisdizionale del citato IOB, evidenziata già in Bucalo 2022, p. 270 ss.; Stiano 2022, p. 1034 ss., che rimarca la tendenza in atto – tipica del diritto internazionale – alla condivisione del potere tra Stati e soggetti non-statali; Buratti 2022, p. 31 ss., che evidenzia come l'IOB somigli in parte ad uno strumento di risoluzione alternativa delle controversie ed in parte ad un servizio aziendale di gestione dei reclami; Iannotti della Valle 2021, p. 144 ss., che evidenzia come le forme di giurisdizione privata testimonino la evidente crisi della sovranità statale e, con essa, della giurisdizione; Bonini 2020, p. 265 ss., che si chiede se l'IOB di Facebook costituisca prototipo di un nuovo tipo di Corte.
54. Cfr. D'Ippolito 2021.
55. Si pensi, ad esempio, al caso *Cambridge Analytica*, sul quale si segnala l'interessate intervento di G. Scorza (componente del Collegio del Garante Privacy), v. Scorza 2023.
56. Per la cui ricostruzione, si rinvia alle riflessioni di Niro 2023, p. 253 ss., che evidenzia come i criteri di moderazione adottati siano "non solo stabiliti in forma unilaterale, ma anche altamente discrezionali, così da consentire decisioni differenziate, caso per caso", così finendo per stabilire "dove vada tracciato il confine tra discorso politico e discorso d'odio, quali immagini configurino il diritto di cronaca e quali il compiacimento dell'osceno […] in un'ottica di massimizzazione del profitto […] a prescindere da ogni riferimento ad eventuali limiti fissati dalle Leggi fondamentali dei Paesi in cui esse operano".
57. Nonostante Internet nasca come strumento "decentralizzato e orizzontale" (Flick–Flick 2022, p. 108), infatti, i servizi più diffusi hanno assunto una evidente propensione oligopolistica, anche perché l'analisi dei c.d. *Big Data* richiede capitali e infrastrutture di non poco conto.
58. Si pensi, *inter alia*, allo scontro del 2020 tra Donald Trump e Twitter (Vigorito 2020), che ha visto la piattaforma intervenire in merito a possibili messaggi di disinformazione, ed il Presidente replicare con un ordine esecutivo asseritamente finalizzato a garantire la massima libertà di espressione del pensiero, prevedendo – in deroga alla sez. 230 del *Communications Decency Act* del 1996 (successivamente ripristinata da Joe Biden) – ipotesi di responsabilità per i social che esercitino attività di moderazione di contenuti fake (cfr. Posteraro 2020). E ancora alla chiusura del profilo Twitter dell'ex Presidente USA nel 2021, per ripetute violazioni del codice di buona condotta applicabile a tutti gli utenti del servizio. Sul tema di segnalano anche: Manetti 2021, p. 194 ss.; Bertolini 2021, p. 1271 ss.
59. Monti 2022, p. 199 ss., che richiama la pronuncia CGUE C-131/12 del 13 maggio 2014, la decisione della Corte costituzionale tedesca 6 novembre 2019, 1 BvR 276/17, par. 105, nonché alcune sentenze del Tribunale di Roma

sorta di libertà di espressione degli attori digitali, che intenderebbe superare l'inquadramento del fenomeno in termini meramente privatistici, per avvicinarlo ad una dimensione pubblicistica analoga a quella delle comunità intermedie di cui all'art. 2 Cost.[60]. In entrambi i casi, con il rischio di creare ordinamenti giuridici autonomi rispetto a quelli statali, in grado di implementare una sorta di "diritto senza Stato"[61].

3. Oltre le *private policies*: dal *soft law* al DSA

L'Unione europea, dinanzi agli evidenti mutamenti nelle modalità d'interazione tra individui, preso atto dell'inadeguatezza delle regolamentazioni tradizionali (sviluppate prima delle innovazioni di cui si è parlato), ha adottato una più attenta strategia di regolamentazione dei fenomeni, dapprima mediante strumenti di *soft law* e, solo successivamente, attraverso una disciplina più rigorosa, ma anche (opinabilmente[62]) ipertrofica.

La prima fase di tale percorso si è caratterizzata per risoluzioni e comunicazioni (soft law) degli organi dell'Ue, tra le quali – senza pretesa di esaustività – si segnalano: la Risoluzione del Parlamento europeo del 15 giugno 2017 sulle piattaforme online e il mercato unico digitale[63]; la Comunicazione della Commissione del 26 aprile 2018 intitolata "Contrastare la disinformazione online: un approccio europeo"[64] e la Comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 5 dicembre 2018 intitolata il "Piano d'azione contro la disinformazione"[65]; senza dimenticare – in ambito di hate speech – la Decisione Quadro 2008/913/GAI del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.

Sempre in relazione alla prima fase, va ricordata l'adozione di codici di autoregolamentazione, ai quali hanno aderito le piattaforme[66], e precisamente: il "Code of Conduct for countering illegal hate speech online" del 2016[67] (che impone, nella maggior parte dei casi, la rimozione dei contenuti di odio entro 24 ore dalla segnalazione degli stessi); il "Code of Practice on Disinformation" del 2018 (aggiornato nel 2022, post epidemia Covid-19)[68], che prevede (a carico di motori di ricerca e social network) l'individuazione di pagine web non attendibili, incentivi alla rimozione di profili

sull'esclusione di contenuti pubblicati sui social da Forza Nuova e Casa Pound (trattasi di ord. Trib. Roma sez. impresa 12 dicembre 2019, che ha escluso contenuti prodotti su Facebook da Forza Nuova, e di ord. Trib. Roma, sez. diritti della persona, 23 febbraio 2020, che ha invece riammesso i contenuti pubblicati da Casa Pound, evidenziando la peculiare posizione di Facebook, esaminate da Grandinetti 2021, p. 173 ss., ma anche – più di recente – da Vigevani 2023, p. 142 ss.), citando infine l'interessante lavoro di Caruso 2020.

60. In tal senso, Allegri 2018, p. 29.

61. Espressione mutuata da Cremona 2023, p. 48 ss.

62. Si segnala, a tal riguardo, Raffiotta 2023, p. 245 ss., che evidenzia come la sovrapposizione di tante normative eurounitarie (GDPR, Data Act, Data Governance Act, NIS, DMA, DSA, ecc.) finisca anche per pregiudicare la competitività delle imprese europee; solleva ulteriori perplessità, con specifico riferimento al DSA, Sgueo 2023, p. 746 ss.; per un tentativo di ricostruzione delle interazioni tra DSA e altri fonti in ambito digitale, si segnala anche Michinelli 2023, p. 29 ss., che parla di vero e proprio "puzzle".

63. Risoluzione 2016/2276(INI), pubblicata in GU C 331 del 18 settembre 2018.

64. COM(2018) 236.

65. JOIN/2018/36.

66. Abbondante 2017.

67. Al Codice hanno aderito: Facebook, Microsoft, Twitter e YouTube nel 2016; Instagram, Snapchat e Dailymotion nel 2018; Jeuxvideo.com nel 2019; TikTok nel 2020; LinkedIn nel 2021; Rakuten Viber e Twitch nel 2022. Sul tema si segnala Casarosa 2020; sui rapporti di tale codice con il DSA si sofferma Vasino 2023, p. 130 ss.; il tema è preso in esame, di recente, anche da Punzi 2024, p. 457 ss.

68. Dapprima (nel 2018) Facebook, Google, Mozilla, Twitter, Microsoft e Tik Tok, per poi giungere a ben 44 sottoscrittori al 2 aprile 2024 (cfr. Commissione europea 2022). Sul tema si segnalano: Monti 2019, p. 320 ss.; Pagano 2019, p. 8s s.; Monti 2020, p. 282 ss.

social falsi e di notizie non vere, maggiore trasparenza nei finanziamenti sottesi alla diffusione di informazioni, agevolazione all'accesso a diverse fonti di informazione.

È indiscutibile che tali iniziative, seppur con i limiti connaturati all'adozione di strumenti non vincolanti, abbiano il merito di avere reso maggiormente omogeneo il trattamento di fenomeni che, in ambito Ue e USA, venivano inquadrati in modo decisamente diverso, giungendo finanche all'adozione di provvedimenti dall'eco mediatica clamorosa, in precedenza inimmaginabili, specie ove si consideri che gli stessi hanno riguardato il Presidente (allora uscente) degli Stati Uniti[69].

D'altro canto, è altrettanto evidente che l'attribuzione di un potere di moderazione così ampio a soggetti privati, in assenza di un quadro regolamentare chiaro e ben definito, implichi l'esercizio di un potere di "censura privata" con modalità non sempre univoche, condizionato anche – alla luce del rischio di applicazione di sanzioni economiche – dall'adozione di politiche talvolta eccessivamente prudenziali, che travalicano il reale obiettivo dei codici di condotta, per ridurre al minimo il rischio di applicazione di eventuali sanzioni economiche. E ciò, si badi, da parte di soggetti privati che neanche sono inquadrabili quali editori, ma che esercitano prerogative assai simili[70], pur non essendo sottoposti ad analoghe responsabilità.

In un contesto di tal tipo, reso ancor più critico dall'epidemia Covid-19 del 2020[71] e dal conflitto tra Russia e Ucraina del 2022[72], nella consapevolezza che la vita dell'uomo dipenda sempre più da Internet e dalle web companies[73], l'Ue sta tentando di assumere un ruolo di riferimento a livello mondiale[74], provando a disciplinare i fenomeni correlati alla trasformazione digitale mediante nuovi strumenti di co-regolazione[75].

Ne sono prova il rinnovato "Code of Practice on Disinformation" del 2022[76] e le plurime normative settoriali (Digital Services Act – DSA, Digital Markets Act – DMA, Data Governance

69. Si pensi all'esclusione di Donald Trump da alcuni social network, per aver contribuito con i propri discorsi all'assalto al Capitol Hill del 2021, all'esito della vittoria di Biden alle elezioni presidenziali (sul tema, si rinvia alle precedenti note nn. 55 e 60).
70. Si pensi alle attività di *fact-checking* e rimozione di pagine di disinformazione.
71. Che ha spinto all'adozione della comunicazione JOIN(2020) 8, cit. in nota 29, volta a contrastare la disinformazione mediante diffusione di maggiori informazioni in favore dei cittadini, rafforzamento della trasparenza delle piattaforme, piena attuazione dei codici di autoregolamentazione e sostegno ai "fact-checkers".
72. Cfr. Nicastro 2023.
73. Cfr. Kowalicka 2022, p. 341 ss.
74. Si segnala, in tal senso, quanto affermato nella Comunicazione della Commissione, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM/2021/118, che ha individuato quattro punti cardinali, i primi due incentrati sulle capacità digitali a livello di infrastrutture e di istruzione e competenze, mentre gli altri due sulla trasformazione digitale delle imprese e dei servizi pubblici, con lo scopo di delineare "un percorso chiaro verso una visione e azioni comuni che l'Europa dovrà seguire per avere successo nel decennio digitale, a livello dell'Unione ma anche nel mondo".
75. Visto il tentativo di coinvolgere gli stakeholders nell'elaborazione dei principi e delle direttive in materia. Sul tema, si segnala Simoncini 2022, p. 1031 ss., che spiega tale tendenza alla luce della crisi sempre più evidente dell'efficienza amministrativa delle organizzazioni pubbliche, della crescente dipendenza collettiva da beni e servizi offerti dalle grandi corporazioni tecnologiche private e, infine, della profonda asimmetria informativa tra regolatore pubblico e destinatari della regolazione digitale, che spesso rende i costi regolativi ed amministrativi insostenibili per i destinatari stessi, precisando come la co-regolazione rappresenti una sorta di contromisura messa in atto per evitare una devoluzione di potestà normative ai nuovi "poteri privati".
76. Che intende superare i limiti del precedente codice del 2018 (mediante demonetizzazione dell'informazione, maggiore trasparenza, alfabetizzazione degli utenti, rafforzamento del contrasto alle notizie false, monitoraggio del rispetto degli impegni assunti dai sottoscrittori, ecc.), configurandosi – alla luce dell'entrata in vigore del DSA – come atto di co-regolamentazione (e non più di autoregolamentazione), il cui mancato rispetto sarà sanzionabile dall'Ue. Sul tema si segnala Monti 2022-a.

Act – DGA, Data Act – DA, Artificial Intelligence Act – AIA), che superano le precedenti discipline di soft law e autoregolamentazione, con l'obiettivo di porre la dimensione umana al centro dell'ecosistema digitale[77], favorendo l'implementazione del mercato unico digitale in prospettiva antropocentrica[78].

Per quanto di maggior rilievo ai fini del presente scritto, nell'ottobre del 2022 l'Unione europea ha adottato il DSA[79], che stabilisce nuovi limiti per prevenire la diffusione di contenuti dannosi online, mediante iniziative di mitigazione dei rischi sistemici[80], applicazione di solidi strumenti di moderazione dei contenuti, implementazione di una maggiore trasparenza in relazione ad algoritmi utilizzati, criteri di moderazione e pubblicità, obblighi di rendicontazione sulle iniziative assunte[81] e di rimozione dei contenuti illegali, cui si aggiunge la possibilità per la Commissione di chiedere interventi straordinari in presenza di guerre, atti terroristici, disastri naturali e minacce per la salute.

Nel dettaglio, il DSA intende rafforzare i diritti e creare un ambiente digitale più sicuro[82], regolamentando le attività di intermediari e piattaforme online[83], rivolgendosi sia alle piattaforme di dimensioni minori, sia – con particolare attenzione – a quelle maggiori (VLOSE e VLOP[84]), prevedendo (*inter alia*) obblighi di contrasto alla diffusione di contenuti illegali (anche su indicazione di autorità giudiziarie e amministrative[85]) e di fornire informazioni utili alla repressione di illeciti[86], senza comunque la previsione di un generale obbligo di sorveglianza sulle informazioni che i prestatori trasmettono o memorizzano, o ancora di accertamento attivo dei fatti o delle circostanze che indichino la presenza di attività illegali[87].

Il DSA prende in esame tre tipologie di attività svolte dai prestatori di servizi, consistenti nel semplice trasporto di informazioni, nella loro memorizzazione temporanea per ragioni di maggiore efficienza del servizio e nella loro memorizzazione su richiesta del destinatario di un servizio[88],

77. In termini di protezione dei dati personali, non discriminazione, neutralità tecnologica, inclusività.
78. Davola 2022, p. 239 ss.
79. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (*Regolamento sui servizi digitali*), entrato pienamente in vigore il 17 febbraio 2024. Sul DSA, in chiave generale, si segnalano sia il testo di Bolognini–Pelino–Scialdone 2023, sia la sezione monografica Aa.Vv. 2023, pp. 12-122, nonché i plurimi contributi pubblicati anch'essi su unica rivista, in chiave monografica da: Del Gatto 2023; Finocchiaro 2023; Sgueo 2023. In rapporto alla disinformazione, con spunti di riflessione in vista delle elezioni europee e americane del 2024, si segnala l'interessante contributo di Longo 2023; sempre in ambito di disinformazione, è interessante la disamina di D'Agostino 2023 e di Birritteri 2023; Flaminio 2022. Per alcune riflessioni in tema di anonimato, si veda anche Finocchiaro 2021.
80. Specie se idonei a recare pregiudizio a diritti fondamentali e/o a processi elettorali.
81. Mediante rapporti periodici da inviare alla Commissione Ue.
82. Al punto da aver acquisito la qualifica di "nuova costituzione digitale dell'Unione europea" in Bolognini–Pelino–Scialdone 2023 (*Introduzione*).
83. I mercati digitali, i motori di ricerca, i servizi di comunicazione elettronica, i servizi cloud, i social network, le piattaforme di condivisione di contenuti, i c.d. app store, le piattaforme di viaggi e alloggio online, ecc.
84. *Very Large Online Search Engine* e *Very Large Online Platform*, con oltre 45 milioni di utenti mensili (cfr. art. 33 DSA), pari a circa il 10% dei 450 milioni di consumatori presenti in Europa, tra cui Youtube, Amazon, Instagram, Twitter, Google Search, Google Maps, Google Apps, Bing, Tiktok, Facebook, Wikipedia, Linkedin, Snapchat, ecc.
85. Cfr. art. 9 del DSA.
86. Cfr. art. 10 del DSA.
87. In tal senso dispone l'art. 8 del DSA. Di fatto, la prima parte del DSA disciplina l'esenzione da responsabilità degli intermediari, ricalcando (con poche eccezioni) quanto già previsto dalla direttiva 2000/31/UE.
88. Rispettivamente, artt. 4, 5 e 6 del DSA.

disciplinando per ciascuna di esse i presupposti per l'esenzione da responsabilità.

A tal riguardo, appaiono meritevoli di interesse due particolari fattispecie di esenzione da responsabilità.

La prima di esse – in ipotesi di memorizzazione temporanea di informazioni – è a beneficio del prestatore che "agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso alle stesse, non appena venga effettivamente a conoscenza del fatto che le informazioni all'origine della trasmissione sono state rimosse dalla rete o che l'accesso alle informazioni è stato disabilitato…", e intenderebbe fronteggiare il fenomeno dell'immissione di contenuti in rete da parte di soggetti che – poi – si rendano anonimi o non agevolmente identificabili.

La seconda, invece, riguarda il prestatore che memorizzi informazioni in via non temporanea, che si considera esente da responsabilità ove "a) non sia effettivamente a conoscenza delle attività o dei contenuti illegali e, per quanto attiene a domande risarcitorie, non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti; oppure b) non appena venga a conoscenza di tali attività o contenuti illegali o divenga consapevole di tali fatti o circostanze, agisca immediatamente per rimuovere i contenuti illegali o per disabilitare l'accesso agli stessi", così prevendendosi una forma di "secondary liability" che, pur non introducendo un generalizzato obbligo di monitoraggio dei contenuti (in linea di continuità con il principio di irresponsabilità di cui alla Direttiva sul commercio elettronico 2000/31/CE), impone comunque un obbligo di diligenza qualificata, ove il prestatore del servizio venga a conoscenza dell'illiceità dei contenuti memorizzati.

Accanto a tali previsioni, è altresì previsto che le piattaforme interessate valorizzino il contributo degli utenti: predisponendo meccanismi idonei a consentire la segnalazione di contenuti illegali, di facile accesso e uso (in via elettronica); consentendo la presentazione di segnalazioni esclusivamente per via elettronica; imponendo al prestatore del servizio di notificare al segnalante la propria decisione, che dovrà essere adottata in modo tempestivo, diligente, non arbitrario e obiettivo, rispettando obblighi di chiara e specifica motivazione[89]; prevedendo altresì possibilità di reclamo contro le decisioni adottate, nonché sistemi di risoluzione stragiudiziale delle controversie[90].

Tale impostazione, che potremmo definire – *latu sensu* – di sussidiarietà orizzontale, ripropone strumenti partecipativi già adottati in altre aree del diritto caratterizzate dalla confluenza di interessi pubblici e privati[91], cui si aggiunge la peculiare introduzione dei c.d. "trusted flaggers" (ossia di segnalatori ritenuti attendibili in virtù della propria indipendenza e di comprovate capacità e competenze[92]), le cui segnalazioni vengono esaminate con priorità e decise senza indebito ritardo.

89. Cfr. artt. 16 e 17 del DSA (c.d. meccanismi di "Notice & Takedown").

90. Cfr. artt. 20 e 21 del DSA.

91. Si pensi, senza pretesa di esaustività, alla disciplina della trasparenza di cui al d.lgs. n. 33/2013 e ss.mm.ii., o più di recente alla disciplina del whistleblowing, il cui ambito di applicazione è risultato ulteriormente esteso a seguito dell'adozione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (direttiva recepita in Italia mediante d.lgs. n. 24/2023), che ha incluso nell'obbligo del *whistleblowing*, insieme al settore pubblico, anche tutte le imprese del settore privato che nell'anno precedente hanno impiegato – in media – un numero di lavoratori subordinati pari o superiore a 250.

92. Cfr. art. 22 del DSA, secondo cui "La qualifica di «segnalatore attendibile» a norma del presente regolamento viene riconosciuta, su richiesta di qualunque ente, dal coordinatore dei servizi digitali dello Stato membro in cui è stabilito il richiedente al richiedente che abbia dimostrato di soddisfare tutte le condizioni seguenti: a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo".

Le attività di contrasto alla diffusione di contenuti illegali[93], sulla scorta anche delle segnalazioni ricevute, confluiscono in una relazione annuale sull'attività di moderazione[94].

Accanto a tali iniziative, poi, per le piattaforme di maggiori dimensioni, sono previste delle attività di prevenzione e mitigazione dei c.d. "systemic risks"[95], ossia degli effetti negativi correlati alla diffusione di contenuti illegali rispetto ai diritti fondamentali[96] degli utenti in ambito Ue, cui corrispondono ampi ed incisivi poteri della Commissione europea[97].

In ipotesi di violazione del DSA, sono previste sanzioni fino al 6% del fatturato annuo totale, con ulteriori ammende in caso di presentazione di informazioni errate, incomplete o fuorvianti da parte delle piattaforme, nell'ipotesi di mancata correzione di tali informazioni e di mancata cooperazione durante le ispezioni[98], cui si aggiunge la facoltà per i destinatari dei servizi digitali di richiedere un risarcimento per eventuali danni o perdite subite a causa delle violazioni commesse dalle piattaforme[99].

Pur essendo scontato il giudizio favorevole all'introduzione di una disciplina vincolante ed uniforme per un territorio vasto come quello europeo, permangono diverse perplessità sulla sua concreta efficacia, che potrà essere compiutamente valutata solo nel tempo, all'esito della piena implementazione del DSA, della conclusione dei primi procedimenti di controllo e della verifica dell'impatto del nuovo impianto normativo sull'attività esegetica di chi dovrà assumere (in sede giudiziale e stragiudiziale) le decisioni del caso.

4. Cenni a (e riflessioni su) alcuni casi pratici

Sulla scorta delle osservazioni svolte, al solo fine di coglierne meglio le implicazioni pratiche e senza pretesa di esaustività, si segnalano alcune recenti iniziative e pronunce che hanno esaminato il rapporto tra piattaforme e contenuti tramite di esse diffusi.

La Commissione europea, ad esempio, ha aperto nel 2023 un'indagine nei confronti della piattaforma X (ex Twitter), per possibile violazione del DSA, in relazione alle modalità di trattamento del conflitto tra Palestina e Israele[100], precisando l'intenzione di esaminare i tentativi di X di contrastare la diffusione di contenuti illegali sulla piattaforma,

93. Che possono condurre anche alla sospensione della prestazione di servizi, nei confronti di determinati soggetti che forniscano – con frequenza – contenuti manifestamente illegali.

94. Cfr. art. 55 DSA.

95. Artt. 33 ss. del DSA, rispetto ai quali si segnalano le riflessioni di Palumbo–Piemonte 2023, che esaminano le disposizioni del DSA rispetto alla Carta dei diritti fondamentali dell'Unione europea, rispetto ai principi di legalità e proporzionalità, manifestando perplessità anche in merito alla scelta di attribuire alla Commissione, che è parte del potere esecutivo nell'assetto istituzionale dell'Ue, enormi poteri in materia di libertà d'espressione.

96. Riservatezza, vita familiare, tutela dei minori, protezione della salute, sicurezza pubblica, libertà di informazione e di espressione, libero e consapevole esercizio dei diritti democratici, ecc. (cfr. considerando n. 52 del DSA).

97. Si pensi al disposto dell'art. 36 DSA, secondo cui la Commissione può imporre a piattaforme e motori di ricerca di grandi dimensioni di valutare se i propri servizi contribuiscano a minacce gravi, individuare misure specifiche per prevenire, eliminare o limitare le gravi minacce, chiedendo una relazione sulle citate verifiche e sull'attuazione degli interventi prescritti.

98. Cfr. artt. 52 (per gli Stati membri) e 72 (per la Commissione Ue) del DSA. Il primo articolo citato prevede sanzioni "pari al 6% del fatturato annuo mondiale del fornitore di servizi", disponendo anche per altre sanzioni di tipo economico; il secondo prevede invece "sanzioni pecuniarie non superiori al 6% del fatturato totale realizzato a livello mondiale su base annua dal fornitore", disponendo anche in tal caso diverse tipologie di sanzioni economiche.

99. Cfr. art. 54 DSA, secondo cui "I destinatari del servizio hanno il diritto di chiedere un risarcimento, conformemente al diritto dell'Unione e nazionale, ai fornitori di servizi intermediari relativamente a danni o perdite subiti a seguito di una violazione degli obblighi stabiliti dal presente regolamento da parte dei fornitori di servizi intermediari".

100. In specie, alla luce di segnalazioni di disinformazione diffusa sul conflitto, attraverso una rete di propaganda di dozzine di account che avrebbero condiviso contenuti falsi e provocatori. Cfr. il comunicato stampa *La Commissione avvia un procedimento formale nei confronti di X a norma del regolamento sui servizi digitali*.

esaminando lo sforzo nel fermare la manipolazione delle informazioni tramite il sistema "Community Notes" ed altre politiche[101]. Rispetto a tale iniziativa, si evidenzia come X abbia ribadito il proprio impegno al rispetto del DSA, per creare un ambiente sicuro e inclusivo per tutti gli utenti della piattaforma, proteggendo al tempo stesso la libertà d'espressione[102].

Sempre X, tra il 2023 ed il 2024, è stata al centro dell'attenzione per l'iniziativa di consentire l'acquisto (con una particolare modalità di abbonamento) della c.d. "spunta blu" (che dovrebbe indicare il verificato profilo di personaggi noti)[103], sortendo un effetto assai controverso, che secondo alcuni avrebbe potuto generare maggiore disinformazione, agevolando attività illecite[104], in contrasto anche con il DSA (tenuto conto che chiunque avrebbe potuto abbonarsi al servizio e conseguire lo status di "account verificato")[105].

E ancora, nel maggio del 2023, la Commissione europea ha avviato un'indagine nei confronti di Meta (Facebook – Instagram) in merito a possibili dipendenze create nei minori[106], mentre nel dicembre del medesimo anno la Commissione ha "rammentato" al gestore della piattaforma i precisi obblighi di moderazione dei contenuti previsti dal DSA, con espresso invito a prestare particolare attenzione alle fake news relative al conflitto tra Hamas e Israele, dando comunque atto del maggior impegno di Meta (in termini di misure di mitigazione, cooperazione con le autorità indipendenti, tempi di risposta e fact-checking) e concludendo con l'affermazione secondo cui "The DSA is here to protect free speech against arbitrary decisions, and at the same time protect our citizens and democracies"[107].

Se tali iniziative denotano una sempre maggiore attenzione alla qualità dei contenuti on line e al rischio che gli stessi possano incidere sui diritti fondamentali, non può comunque trascurarsi la tendenza a riconoscere esenzioni di responsabilità per la diffusione, su siti e piattaforme non giornalistiche, di contenuti realizzati da terzi.

È il caso della recente sentenza TAR Lazio n. 1393 del 2024[108], riguardante proprio Meta Platforms Ireland Ltd., ove si afferma che va esente da responsabilità – in relazione ai contenuti memorizzati da terzi sulla rete – il fornitore di servizi di hosting che non è a conoscenza delle attività illecite che avvengono tramite i propri servizi, sempre che, non appena conosciuti tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso, e ciò anche ove dotato di un sistema di controllo automatizzato[109].

101. Pedretti 2023.

102. Il comunicato (post) del 18 dicembre 2023, testualmente, riportava "X remains committed to complying with the Digital Services Act and is cooperating with the regulatory process. It is important that this process remains free of political influence and follows the law. X is focused on creating a safe and inclusive environment for all users on our platform, while protecting freedom of expression, and we will continue to work tirelessly towards this goal".

103. Sul funzionamento delle spunte blu, si segnala l'articolo di Nicolao 2023.

104. Come evidenziato anche da alcune imprese impegnate nella sicurezza digitale (cfr. Titterington 2023).

105. Sul tema, di recente, si legga l'articolo di Iorio 2024. I documenti ufficiali dell'Ue, allo stato, sono reperibili sul sito dell'Unione europea.

106. Cfr. *La Commissione Europea ha avviato un'altra indagine contro Meta per presunte violazioni del Digital Services Act sulla tutela dei minori*, in "Il Post", 16 maggio 2024, che rinvia per i documenti ufficiali a European Commission 2024.

107. Nel dettaglio, il commissario europeo per il Mercato interno e i Servizi Thierry Breton ha pubblicato una formale lettera, datata 11 ottobre 2023 (rinvenibile anche sul Corriere della sera di pari data, nell'articolo di Cané 2023).

108. Cfr. TAR Lazio, Roma, sez. IV, 24 gennaio 2024, n. 1393, in *Guida al diritto*, 2024, 9, p. 86.

109. Non essendo sufficiente il solo fatto che il software contempli l'astratta possibilità, in un numero limitato di casi, di sottoporre una singola inserzione a revisione umana, dovendo tale circostanza essere, al contrario, allegata e dimostrata in concreto per poter ritenere in giudizio che il provider si sia venuto a trovare in una condizione di effettiva conoscenza dell'inserzione illecita, conoscenza idonea a giustificare un addebito a suo carico a titolo di concorso nella commissione dell'altrui illecito.

Nel medesimo senso, va ricordata anche una pronuncia 2021 (ante DSA) della Cassazione[110], secondo cui "In tema di diffamazione, l'amministratore di un sito internet non è responsabile ai sensi dell'art. 57 c.p., in quanto tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, facebook), salvo che sussistano elementi che denotino la compartecipazione dell'amministratore alla attività diffamatoria", nonostante nel caso in esame il titolare del sito Internet avesse condiviso la pubblicazione di un articolo offensivo della reputazione di un agente di polizia, dopo aver collaborato alla raccolta delle informazioni necessarie per la sua redazione, partecipato al collettivo politico che ne aveva elaborato l'idea e rivendicato in dibattimento il contenuto.

È quindi evidente come, al di là delle dichiarazioni di principio, la condizione di neutralità degli intermediari rispetto ai contenuti ospitati, che giustificherebbe l'esenzione da responsabilità, apra la porta a valutazioni discrezionali, che non sempre tengono in debito conto l'effettivo ruolo di chi ospita i contenuti[111], ritenuto di per sé comunque insufficiente a dimostrare la consapevolezza della loro natura illecita (la cui prova è già difficile da fornire[112]), così divenendo inevitabile spostare l'attenzione sulle attività di accountability e – quindi – sulla verifica (anch'essa caratterizzata da margini di discrezionalità) di effettività, adeguatezza e trasparenza in merito agli adempimenti finalizzati alla prevenzione dei rischi sistemici.

5. Considerazioni *in itinere*

Dopo aver passato in rassegna alcuni dei principali aspetti del difficile rapporto tra libertà d'espressione e tecnologie digitali, risulta piuttosto difficile immaginare di stilare delle "conclusioni" che possano davvero ritenersi tali, secondo l'etimologia del termine[113] (che presupporrebbe un'attività che possa dirsi – effettivamente – portata a "compimento"), senza aver prima riallacciato le fila del discorso con alcune considerazioni *in itinere*.

Vi si oppongono – *inter alia* – la mutevolezza del contesto sociale, degli equilibri economico-politici, delle norme adottate ai vari livelli istituzionali e delle correlate interpretazioni, nonché la consapevolezza di un necessario – e quotidiano – monitoraggio, in grado tanto di confermare quanto da smentire ogni ipotetico punto d'arrivo.

Ecco le ragioni che suggeriscono di formulare qualche ultima riflessione, alle soglie di una (possibile) sintesi.

5.1. Una prima riflessione sulle piattaforme

In una Comunicazione del 2016[114] (non troppo distante, in senso assoluto, seppur risalente rispetto ai veloci mutamenti del mondo digitale), la Commissione europea ha affermato che "l'internet del futuro è destinato a fallire se gli utenti non avranno fiducia nelle piattaforme online…": un "modello organizzativo che utilizza un'infrastruttura

110. Cass. pen., sez. V, 12 gennaio 2021, n. 7220, in *MediaLaws*, 2021, 2, p. 247 ss. (con nota di Vimercati 2021).

111. Cfr. Pelino 2023, p. 168 ss., che evidenzia come il ruolo degli intermediari, che agiscono sui contenuti (selezionandoli o escludendoli, valorizzandoli, proponendoli mediante sistemi di raccomandazione, profilando i destinatari, ecc.) difficilmente possa essere considerato neutrale, specie per piattaforme e motori di ricerca di maggiori dimensioni, non a caso obbligati a fronteggiare i rischi sistemici.

112. Ove si tenga in conto il tenore del considerando n. 22 del DSA, secondo cui "Tale conoscenza o consapevolezza effettiva non può essere considerata acquisita per il solo motivo che tale prestatore è consapevole, in senso generale, del fatto che il suo servizio è utilizzato anche per memorizzare contenuti illegali. Inoltre, la circostanza che il prestatore proceda a un'indicizzazione automatizzata delle informazioni caricate sul suo servizio, che il servizio contenga una funzione di ricerca o che consigli le informazioni in funzione del profilo o delle preferenze dei destinatari del servizio non è un motivo sufficiente per considerare che il prestatore abbia una conoscenza «specifica» di attività illegali realizzate sulla medesima piattaforma o di contenuti illegali ivi memorizzati".

113. Dal latino "cum" (con) "claudere" (chiudere).

114. Comunicazione della Commissione *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, COM/2016/0288, 4.

software connessa, con raccolta e analisi dati e applicazione di algoritmi, per mettere in contatto diverse categorie di utenti"[115].

E se ciò è vero in chiave generale, è ancor più evidente in tema di libertà d'espressione, ove si consideri che le nuove tecnologie hanno enormemente potenziato l'esercizio di tale diritto, consentendo a chiunque di diffondere il proprio pensiero a livello globale e alimentando una maggiore democratizzazione dell'informazione, ma anche imponendo di adottare politiche di contrasto alla diffusione di fake news e disinformazione[116], nonché di prendere atto della necessità di un controllo pubblico sull'operato di soggetti privati operanti in regime di oligopolio[117], ricalibrando – come già accaduto in passato – i parametri di bilanciamento tra l'esercizio dei diritti individuali e la libertà d'espressione che, da strumento di democratizzazione[118], sta invece assumendo una tendenza antagonista rispetto ai tradizionali mezzi di informazione, i quali – anzi – risultano progressivamente indeboliti e sempre più sotto attacco[119].

Ed ecco che, se è innegabile che il futuro di Internet dipenda dalla fiducia nelle piattaforme, non sarebbe peregrino ipotizzare forme di moderazione e controllo dei contenuti che siano più incisive anche rispetto a quanto disposto dal DSA, ferma la necessità di scongiurare che l'esercizio del potere di moderazione attribuito alle piattaforme possa diventare una vera e propria censura in mano privata[120], risultando invece indispensabile il coinvolgimento dei pubblici poteri, in virtù della natura degli interessi coinvolti.

Una consapevolezza, questa, che sta maturando anche presso le corti statunitensi, come confermato dalla *concurring opinion* resa nel 2021 dal giudice Thomas (nel caso *Knight Insitute v. Trump*, 593 U.S. 2021)[121], che rimarca come il potere di censura delle piattaforme private, esercitato sulla scorta delle proprie condizioni di servizio, testimoni l'inadeguatezza della regolamentazione vigente, anche alla luce del fatto che il primo emendamento garantisce la libertà d'espressione solo nei confronti dei poteri pubblici e non dei soggetti privati[122], divenuti però anch'essi "poteri", che possiedono enormi quantità di dati e rappresentano ormai il principale strumento di comunicazione interpersonale (operante in regime di esenzione da responsabilità, ai sensi della c.d. *Good Samaritan Clause*[123]), cui si dovrebbero applicare forme di regolamentazione pubblica che ne limitino il potere[124], essendo evidente che le piattaforme private possano mettere a rischio proprio la libertà di espressione che in origine intendevano preservare.

Riconducendo questa riflessione al nostro ordinamento nazionale, occorre osservare come le forme di regolamentazione pubblica dei contenuti non riguardino solo il settore radiotelevisivo (quale

115. In tal senso, Martinelli 2022, p. 291 ss.

116. Pistorio 2023, ove si evidenzia come il disordine informativo, nel 2022, abbia raggiunto vette ineguagliabili, anche in virtù della diffusione degli strumenti di intelligenza artificiale, auspicando interventi legislativi ma, soprattutto, un "addestramento degli utenti" in termini di alfabetizzazione digitale e algoritmica.

117. Cerrina Feroni 2021.

118. Anche attraverso l'implementazione del pluralismo informativo.

119. Come testimonia l'aumento degli attacchi ai giornalisti in ambito globale, richiamato in Commissione Nazionale Italiana per l'unesco 2022.

120. Rischio comunque evidenziato da Monti 2019-a, p. 37; ma anche, più di recente, a valle dell'adozione del DSA, da Lamberti 2023.

121. Su cui si segnalano: Niro 2021; Monti 2021.

122. Come ribadito in *Manhattan Community Access Corp. V. Halleck*, 587 U.S. (2019), ove si afferma che "the Free Speech Clause prohibits only governmental abridgment of speech. The Free Speech Clause does not prohibit private abridgment of speech".

123. Section 230 del *Communication Decency Act*, già in precedenza citata.

124. Come è accaduto per "company towns" (cittadine di proprietà privata, disciplinate da regolamenti aziendali), "common carriers" (compagnie ferroviarie, di telegrafi e di telefoni) e "places of public accommodation" (luoghi e attività – ristoranti, hotel, negozi, teatri, musei, scuole, chiese, ecc. – aperti al pubblico, sottoposti anche a specifiche discipline antidiscriminatorie).

scelta imposta dalla natura "finita" dello strumento di comunicazione utilizzato[125]), ma anche settori che – di per sé – non si caratterizzano per un'astratta limitatezza di canali e/o frequenze, come il teatro (sin dall'epoca liberale) e il cinema (a partire dal regime fascista), alla luce della particolare capacità suggestiva degli strumenti citati e della propensione ad una fruizione collettiva[126]. Elementi che, osservando bene, sono presenti anche nelle piattaforme digitali, spesso in competizione tra loro mediante la diffusione di contenuti sensazionalistici, idonei ad attirare l'attenzione degli utenti[127] e a diventare virali in tempi rapidissimi.

Ed ecco, quindi, che ci sarebbe da riflettere sulla previsione di forme di responsabilità analoghe a quella editoriale anche per le piattaforme, tenendo conto che, se una piena responsabilità editoriale si giustifica alla luce dell'opera di selezione dei contenuti effettuata in via preventiva dalle imprese editoriali, una responsabilità per certi versi "simile" possa giustificarsi tanto in conseguenza dell'omissione di adeguate iniziative in merito alla diffusione di contenuti "anomali" di cui la piattaforma sia venuta a conoscenza (aspetto disciplinato anche dal DSA), tanto in considerazione della natura stessa delle piattaforme e delle sottostanti dinamiche di funzionamento, che di per sé non possono considerarsi davvero "neutre" rispetto ai contenuti diffusi.

Ciò che si intende dire, in sostanza, è che la distinzione tra "content provider" (chi crea il contenuto e ne è responsabile) e "service provider" (chi fornisce il servizio di ricerca del contenuto o lo ospita, risultando tendenzialmente esente da responsabilità) non risponde più alla reale dinamica digitale, salvo rare e marginali eccezioni.

Basti rileggere, per rendersi conto dell'anomalia, quanto indicato nel considerando n. 42 della Direttiva 2000/31/CE (i cui principi hanno ispirato anche il DSA), secondo cui "Le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate".

Ebbene, sostenere che le attuali piattaforme si limitino ad un processo tecnico di accesso alla rete, per rendere più efficiente la trasmissione delle informazioni, svolgendo un'attività di tipo tecnico-automatico-passivo, senza conoscere le informazioni trasmesse e memorizzate, equivarrebbe a negare del tutto l'esistenza di algoritmi, profilazioni, sistemi di raccomandazione, ecc., oltre che degli ulteriori risvolti economico-pubblicitari di tali meccanismi, di cui pure la giurisprudenza eurounitaria si è ripetutamente occupata[128].

Non è un caso, del resto, che lo stesso DSA distingua operatori di hosting passivo (che offrono il semplice trasporto dei contenuti, ovvero uno spazio di archiviazione, senza interferire nel loro trattamento) e di hosting attivo (che invece selezionano, promuovono, moderano e gestiscono i contenuti[129]), prevedendo per questi ultimi maggiori obblighi[130].

125. Che, come noto, preclude la libertà di accesso e diffusione di ogni possibile messaggio.

126. Cfr. Caretti–Cardone 2019, p. 271 ss.

127. Michael H. Goldhaber, già negli anni Novanta, parlava di una transizione dall'economia "material-based" a quella basata sull'attenzione umana (sul tema si segnala il saggio *Economia dell'attenzione e manipolazione digitale*, in www.stroncature.com, 9 settembre 2024).

128. Si rinvia, per approfondimenti, alla rassegna contenuta in Pollicino 2022, p. 344 ss.

129. In tal senso, in ambito di tutela del diritto d'autore, si veda Cass. civ. sez. I, 13 dicembre 2021, n. 39763, in *AIDA* 2022, 1, p. 792, secondo cui "L'hosting provider attivo è il prestatore dei servizi della società dell'informazione che svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone invece in essere una condotta attiva concorrendo nella commissione dell'altrui illecito, onde resta sottratto al regime di esenzione previsto all'art. 16 d.lg. n. 70/2003".

130. Obblighi già esaminati, con maggiore dettaglio, nel par. 3 che precede, che vanno dalla trasparenza sui meccanismi di moderazione alle informazioni sugli algoritmi di raccomandazione, dalle politiche di gestione

Passando, poi, dal profilo operativo-strutturale a quello funzionale, non può sfuggire come ormai l'informazione circoli più attraverso i giganti del web, che non attraverso gli strumenti di comunicazione tradizionali.

E anche tale aspetto va tenuto in debito conto, poiché il controllo sui contenuti ordinariamente svolto in ambito editoriale non risponde solo ad una necessità correlata alla natura "finita" degli strumenti presi in considerazione, ma mira anche a tutelare valori richiamati nelle principali Carte e Dichiarazioni internazionali (come il diritto ad una informazione attendibile e pluralistica, il rispetto della dignità umana, il divieto di discriminazione, la centralità della persona, ecc.), che devono conformare anche la realtà digitale[131], tenuto conto che la libertà d'espressione si caratterizza sia per una dimensione individuale (maggiormente valorizzata in rete, grazie alla presenza di intermediazioni più incentrate sui profili strutturali[132] che su quelli contenutistici[133]), sia per una dimensione collettiva/sociale[134], che non dovrebbe ammettere derive anarchiche[135].

Anche alla luce di tali aspetti, il DSA rimarca la centralità dei diritti fondamentali, chiarendo sin dal suo primo articolo che "l'obiettivo del presente regolamento è contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta…".

È proprio alla luce di tali consapevolezze (sul reale funzionamento delle piattaforme e sui correlati rischi per le persone), che il legislatore eurounitario avrebbe potuto spingersi oltre, introducendo più incisivi profili di *liability*, così rimettendo in discussione alcuni principi – potenzialmente ostativi all'estensione di responsabilità.

5.2. Note sulla possibile previsione di una responsabilità simil-editoriale: dai casi Uber e Airbnb alla valorizzazione dell'hosting attivo

Nonostante le osservazioni sul reale funzionamento delle piattaforme appaiano difficilmente controvertibili, ciò non toglie che l'estensione di una responsabilità simil-editoriale (nei termini di cui si dirà) alle maggiori piattaforme di comunicazione possa scontrarsi con una equiparazione tra le due categorie di operatori preclusa dal generale divieto di sorveglianza sui contenuti (riproposto, con lievi modifiche, anche dal DSA), ma difficile

dei contenuti illeciti e di protezione degli utenti rispetto a contenuti dannosi alla predisposizione di meccanismi di segnalazione, includendo forme di cooperazione con le Autorità di regolamentazione, valutazione dei rischi sistemici ed altro ancora.

131. In tal senso, si legga l'art. 1 della Dichiarazione dei diritti in Internet del 2015, secondo cui "1. Sono garantiti in Internet i diritti fondamentali di ogni persona riconosciuti dalla Dichiarazione universale dei diritti umani delle Nazioni Unite, dalla Carta dei diritti fondamentali dell'Unione Europea, dalle costituzioni nazionali e dalle dichiarazioni internazionali in materia. 2. Tali diritti devono essere interpretati in modo da assicurarne l'effettività nella dimensione della Rete. 3. Il riconoscimento dei diritti in Internet deve essere fondato sul pieno rispetto della dignità, della libertà, dell'eguaglianza e della diversità di ogni persona, che costituiscono i principi in base ai quali si effettua il bilanciamento con altri diritti". Analogamente, si legga il Capitolo I della Dichiarazione europea sui diritti e principi digitali per il decennio digitale, COM(2022)28 del 26 gennaio 2022, secondo cui "1. Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali".

132. Per la necessità che vi siano costosissime infrastrutture, che solo i giganti della tecnologia sono in grado di implementare (interessante, in tal senso, la qualificazione delle Big Tech come "advertising companies and middlemen in the flow of information", in Albertini 2020, p. 25, nota 70).

133. Cfr. Frosini 2020, che rimarca la natura "open network" delle reti.

134. Vigevani 2021, pp. 162-163, che individua tra i possibili limiti alla libertà d'espressione, non a caso, anche l'ordine pubblico, la tranquillità pubblica, la difesa della patria, la sicurezza, l'ordine economico, ecc.

135. Sul tema, si segnala anche Rodotà 2012.

da affermare anche alla luce dei principi affermati dalla CGUE nei casi Uber e Airbnb.

Quanto al primo aspetto, non può infatti trascurarsi la scelta del legislatore comunitario che – sia con la c.d. direttiva e-commerce del 2000 che con il DSA del 2022 – ha inteso limitare le responsabilità degli Internet services providers (anche "ISP")[136], superando così orientamenti giurisprudenziali ondivaghi (che in alcune occasioni avevano equiparato ISP e content provider, applicando ai primi gli stessi obblighi di controllo e le stesse responsabilità degli editori[137]) e vietando l'introduzione di un obbligo di controllo di tipo generalizzato, limitandosi ad introdurre (con il DSA) maggiori vincoli, senza tuttavia stravolgere il quadro di esenzione da responsabilità dei prestatori di servizi intermediari[138].

Quanto al secondo aspetto, si ritiene interessante rileggere i principi enunciati dalla CGUE per decidere se le piattaforme Uber e Airbnb risultassero o meno equiparabili agli operatori professionali dei rispettivi settori[139]. Nel dettaglio, per Uber (CGUE C-434/15 del 20 dicembre 2017) si è affermato che la piattaforma non si limitasse a mettere a disposizione di autisti ed utenti un "luogo" digitale in cui incontrarsi, svolgendo invece un ruolo organizzativo (al pari delle società di settore) ed offrendo un servizio misto (digitale su piattaforma e analogico in auto) con influenza decisiva sulle condizioni della prestazione, al punto da ritenere indissolubili i servizi on-line e reale. Per Airbnb (CGUE C-390/18 del 10 agosto 2018), invece, seguendo i medesimi criteri di giudizio (c.d. "Uber-test") è stata accertata l'assenza di influenza decisiva, così ritenendo che i servizi offerti in regime misto (digitale e fisico) fossero indipendenti tra loro ed escludendo che la piattaforma fosse quindi assimilabile ad un'agenzia immobiliare.

Ebbene, applicando il medesimo "Uber-test" al possibile parallelo tra piattaforme e mass media tradizionali, emergono due aspetti: il primo di essi è che le piattaforme utilizzate per diffondere disinformazione e discorsi d'odio forniscono un servizio solo digitale e non misto (come molti – ma non tutti i – mass media); il secondo è che le piattaforme – a differenza dei mass media – non sembrano esercitare una "influenza decisiva" sui contenuti pubblicati, concentrandosi più sui destinatari (fruitori) dei contenuti che sui loro produttori (mediante l'indicizzazione, la profilazione, i meccanismi di raccomandazione, l'utilizzo dei dati raccolti per finalità pubblicitarie e/o di espansione in altri settori, ecc.), in linea con le dinamiche della c.d. economia dei dati. Non sembra possibile, pertanto, procedere ad una parificazione di responsabilità che sia fondata sull'equiparazione di funzioni e ruoli.

Sarebbe forse il caso, allora, di valorizzare maggiormente la figura dell'hosting attivo (che indicizza e ottimizza i contenuti, rendendone possibile la ricerca e ricollegandovi contenuti pubblicitari[140]), che più si adatta a realtà digitali le quali, pur non

136. Cfr. Enciclopedia Treccani, *voce "ISP"*, secondo cui ISP è "Sigla di Internet service provider, operatore commerciale che, mediante l'uso di appositi computer con funzioni di server, fornisce ai suoi utenti la possibilità di accedere a Internet e di gestire un proprio sito e proprie caselle di posta elettronica".

137. Per una rassegna degli orientamenti giurisprudenziali, prima della Direttiva 2000/31/CE, si rinvia a Imbruglia 2022, p. 149 ss., che richiama (a favore della equiparazione) la tesi di Trib. Napoli 8 agosto 1997, in *Giust. civ.*, 1998, p. 259 ss., dando atto anche dell'orientamento di senso opposto.

138. Si pensi, *inter alia*, al disposto dell'art. 7 del DSA, secondo cui la volontaria adozione di misure volte e rimuovere contenuti illegali o a disabilitarne l'accesso non impedisce l'accesso al beneficio dell'esenzione da responsabilità *ex* artt. 4, 5 e 6 del DSA. O ancora al chiaro contenuto dell'art. 8 del DSA, che rimarca l'assenza di obblighi generali di sorveglianza o di accertamento attivo di fatti o circostanze che indichino la presenza di attività illegali.

139. Per la cui disamina si rinvia a Canepa 2023, p. 443 ss.

140. Pollicino 2022, p. 349 ss., che cita a tal riguardo la pronuncia Trib. Milano 7 giugno 2011 e 9 novembre 2011, salvo poi evidenziare il superamento dei principi ivi affermati, in C. App. Milano 7 gennaio 2015 e Cass. 21 febbraio 2019, n. 7708. Nel senso di valorizzare il servizio di posizionamento pubblicitario e l'ottimizzazione della presentazione delle offerte di vendita, per la qualificazione del provider come attivo, si segnalano anche CGUE, *Google France*, C-236/08, §118 e CGUE, *L'Oreal*, C-324/09, §123. Per un'analisi della giurisprudenza nazionale sull'host provider attivo, si segnala anche Imbruglia 2022, p. 159 ss.

sovrapponendosi del tutto ai tradizionali mezzi di comunicazione, operano comunque quali gestori di contenuti, della cui diffusione dovrebbero assumere – quantomeno parzialmente – la responsabilità.

In tale direzione sembrerebbe voler deporre anche il considerando n. 18 del DSA, secondo cui – con formula incerta, non vincolante e mal coordinata con agli artt. 7 e 8 del medesimo regolamento – le esenzioni dalla responsabilità: "non dovrebbero" applicarsi allorché, anziché limitarsi a una fornitura neutra dei servizi, l'intermediario svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni; "non dovrebbero" essere disponibili per quanto riguarda la responsabilità relativa alle informazioni fornite non dal destinatario del servizio ma dallo stesso prestatore del servizio intermediario, anche nel caso di informazioni elaborate sotto la "responsabilità editoriale" di tale prestatore.

Rispetto a tale scenario, non va trascurato come l'attribuzione di maggiori responsabilità sia ammissibile anche in assenza di equiparazione formale delle piattaforme ai media professionali, come confermato da alcune recenti normative di settore, che hanno previsto responsabilità del provider per la condivisione di contenuti coperti dal diritto d'autore (Direttiva UE/2019/790), maggiori tutele per i minori anche sulle piattaforme di condivisione video (Direttiva UE/2018/1808[141]), obblighi di controllo preventivo (come per gli editori) sui contenuti terroristici diffusi mediante piattaforme (Regolamento UE/2021/784), norme specifiche sui contenuti di natura politica (Regolamento UE/2024/900), il tutto in conformità ai principi già esposti nel considerando n. 47 della Direttiva 2000/31/CE[142] e nel considerando n. 30 del DSA[143].

Quanto esposto dimostra che, ove gli interessi in gioco lo richiedano, la regola dell'esenzione da responsabilità delle piattaforme, fondata sulla loro proverbiale (e ormai surreale) neutralità, possa venir meno.

Partendo da tale considerazione, viene spontaneo porsi più di un quesito.

Il primo di essi è se la disinformazione e i discorsi d'odio, per la propria capacità di incidere sulle dinamiche democratiche e sui diritti fondamentali delle persone (interessi del tutto assimilabili, per importanza, a quelli che hanno legittimato l'adozione delle normative speciali sopra citate) meritino un intervento legislativo più incisivo rispetto a quanto di recente fatto in ambito eurounitario, e se tale intervento risulti meglio collocato all'interno del DSA o in altra normativa speciale.

La risposta potrebbe ricevere positivo riscontro per il primo aspetto (l'opportunità di un inasprimento della disciplina sulle responsabilità), mentre maggiori dubbi porrebbe l'interrogativo sulla collocazione normativa, tenuto conto che: da una parte il DSA ha una "vocazione" orizzontale (confermata anche dello strumento regolamentare adottato), che suggerirebbe un approccio cauto, in vista dell'applicazione generale a numerosissimi segmenti del mondo digitale; dall'altra, la scelta di collocare eventuali disposizioni più incisive in separati *corpora* rischierebbe di creare problemi di coordinamento tra norme, senza perseguire adeguatamente l'obiettivo di semplificazione interpretativa di cui si sentiva (e si sente ancora) il bisogno.

Il secondo quesito riguarda invece l'individuazione delle possibili caratteristiche di una responsabilità simil-editoriale, che dovrebbe essere in grado di bilanciare al meglio la protezione dei diritti fondamentali e la centralità delle persone con i legittimi interessi di cui sono portatori le piattaforme (attività d'impresa, massima diffusione dei pensieri, ecc.), tenendo peraltro conto che mentre i controlli delle imprese editoriali vengono effettuati in via preliminare, quelli delle piattaforme – anche per evitare fenomeni di vera e propria censura – avrebbero natura di regola successiva.

A tal riguardo, non sarebbe del tutto peregrino ipotizzare meccanismi di tutela più efficaci, quali l'inversione dell'onere della prova[144] della

141. Sul tema, si rinvia anche a Aria 2021.

142. Secondo cui "Gli Stati membri non possono imporre ai prestatori un obbligo di sorveglianza di carattere generale. Tale disposizione non riguarda gli obblighi di sorveglianza in casi specifici…".

143. Secondo cui "I prestatori di servizi intermediari non dovrebbero essere, né de iure né de facto, soggetti a un obbligo di sorveglianza di carattere generale. Ciò non riguarda gli obblighi di sorveglianza in un caso specifico…".

144. Secondo dinamiche già applicati in altri contesti (infortuni sul lavoro, disciplina sulla legittimità dei licenziamenti, responsabilità da custodia o medica, responsabilità del proprietario di animali *ex* art. 2052 cc., ecc.), a

conoscenza dell'attività e/o del contenuto illegittimi, o forme – anche presuntive, salvo prova contraria[145] – di concorso di responsabilità (se non addirittura di solidarietà passiva) in capo tanto al content provider quanto al service provider.

In merito all'inversione dell'onere della prova, si potrebbe chiedere agli operatori digitali di maggiori dimensioni[146], per andare esenti da responsabilità, di dimostrare di aver assunto ogni opportuna precauzione rispetto al monitoraggio di attività e/o contenuti critici, così rafforzando le posizioni degli utenti, spesso non in grado di dimostrare (visto il complesso funzionamento delle piattaforme e dei correlati algoritmi) l'elemento colposo in capo alle proprie controparti digitali. Si riprodurrebbe, in sostanza, un meccanismo già in uso per la tutela dei consumatori rispetto all'acquisto di prodotti difettosi, la cui disciplina non impone all'acquirente di dimostrare la preesistenza del vizio rispetto all'acquisto, chiedendo invece al produttore (alla luce delle proprie competenze e della conoscenza del prodotto interessato) di fornire la prova contraria.

Permarrebbe poi la distinzione rispetto agli editori, ai quali non è consentito di fornire prova contraria in merito a contenuti già preventivamente esaminati, mentre l'inversione dell'onere probatorio costituirebbe un equo bilanciamento rispetto ad un controllo effettuato solo *ex post*.

Anche il riconoscimento di forme di concorso di colpa tra gli operatori di maggiori dimensioni e i creatori/promotori di attività e contenuti illeciti non farebbe altro che prendere atto della natura *latu sensu* gestoria – e non neutra – delle principali piattaforme, così estendendo oltre gli attuali limiti una forma di responsabilità che già è prevista per l'ipotesi in cui il prestatore di servizi non abbia provveduto all'immediata rimozione dei contenuti illeciti o abbia continuato a pubblicarli, nonostante la intervenuta conoscenza dell'illecito o la sua ragionevole verificabilità[147], estendendo proprio tale ultimo campo di azione.

Tale scelta, peraltro, si giustificherebbe in considerazione del fatto che i contenuti illeciti, per quanto non direttamente creati dalle piattaforme, né ufficialmente esaminati in via preventiva, sono comunque già analizzati (anche per fini di raccomandazione) da algoritmi di vario genere[148] che consentono di affermarne (salvo prova contraria) un'astratta conoscibilità, e ciò sia attraverso l'analisi della mera terminologia utilizzata dagli autori (spesso aggressiva e/o discriminatoria), sia attraverso la verifica del traffico dati e della circolazione dei contenuti, che assumono frequentemente (specie per le *fake news*) caratteristiche anomale e/o virali.

Da ultimo, va evidenziato come le analisi algoritmiche volte alla verifica dei contenuti (nei termini e limiti indicati) risulterebbero coerenti anche con il disposto dell'art. 22 del GDPR[149], poiché non si concluderebbero con una decisione automatizzata di "censura", ma consentirebbero di avviare un controllo e una decisione umani in tempi ragionevolmente brevi (che rileverebbero anche quale prova di "diligenza"[150] utile all'esclusione

tutela della posizione del soggetto danneggiato e/o di categorie ritenute deboli (si pensi alla denuncia dei vizi di un prodotto, in ambito di normativa sui consumatori).

145. Già applicate, ad esempio, nei sinistri stradali, rispetto ai quali si presume pari responsabilità dei conducenti coinvolti, salvo prova contraria (art. 2054 co. 2 c.c.).

146. Poiché soggetti economicamente forti e in grado di organizzare adeguati controlli dei contenuti, già in essere per profilazione, raccomandazioni e scopi imprenditoriali.

147. Cass. civ., 19 marzo 2019, n. 7708, in *Nuova giur. civ.*, 2019, n. 5, p. 1049 (con nota di Tormen 2019).

148. Sul tema, in rapporto alle fake news, si segnala Marchetti 2020, p. 29 ss., che evidenzia come gli algoritmi possano sia agevolare sia contrastare la diffusione di notizie false.

149. Secondo il cui co. 1 "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".

150. Diligenza cui fa cenno – fermo il regime delle esenzioni di responsabilità – anche il considerando n. 26 del DSA, secondo cui "Al fine di garantire la certezza del diritto e non scoraggiare le attività volte a individuare, identificare e contrastare i contenuti illegali che i prestatori di tutte le categorie di servizi intermediari intraprendano su base volontaria, è opportuno chiarire che il semplice fatto che i prestatori intraprendano tali attività

di responsabilità), fermo l'obbligo di motivazione specifica di cui all'art. 17.3 lett. c) del DSA[151].

5.3. Un passo indietro: dai pensieri ai contenuti

Alla luce delle considerazioni esposte, si ritiene auspicabile (ed indispensabile, risultando del tutto inadeguata la dimensione di intervento dei singoli Stati, cui resta ben poco in termini di sovranità digitale[152]) un nuovo slancio del legislatore eurounitario, che consenta di contrastare in modo più efficace alcune delle distorsioni sin qui evidenziate, partendo dalle dinamiche sociali e dalla responsabilizzazione degli utenti, prima ancora che dalle politiche sanzionatorie.

Nella consapevolezza che non sia facile individuare interventi che fronteggino efficacemente la disinformazione e la diffusione di discorsi d'odio, si ritiene comunque utile ipotizzare l'individuazione di un criterio di metodo, che tenga conto della reale origine dei contenuti, i quali nascono fuori dalla rete, nel mondo reale, in conseguenza dello scarso valore attribuito alle parole stesse, rispetto al quale non ci si può limitare ad una mera (anche duramente critica[153]) presa d'atto, risultando invece necessario riflettere su quali possano effettivamente essere gli ulteriori strumenti di un auspicabile miglioramento dello *status quo*.

Ed ecco, quindi, che pare possibile operare una razionalizzazione di massima degli interventi da adottare, ricollegandoli alle principali fasi che caratterizzano la diffusione di contenuti on-line: l'elaborazione dei pensieri (prima che diventino contenuti) e l'interazione dell'utente con la rete, che si pongono a monte rispetto ai controlli esperibili dalle piattaforme e all'accertamento di eventuali responsabilità.

In merito all'elaborazione dei pensieri, pur nella consapevolezza della necessità di azioni di educazione/alfabetizzazione digitale e di sensibilizzazione sulla disinformazione e sui discorsi d'odio, va considerato che tali iniziative – stando a quanto verificato in diverse ricerche – sembrano avere efficacia minima, se non addirittura controproducente[154] per la disinformazione, mentre parrebbero avere un'influenza di poco migliore per i discorsi d'odio, che spesso poggiano su una frammentazione sociale cui si dovrebbe tentare di porre rimedio (specie ove si consideri che buona parte degli episodi d'odio riguarda le minoranze di genere, gli orientamenti sessuali e le disabilità[155]), anche valutando l'apposizione di limiti a un diritto fondamentale come la libertà d'espressione[156].

Per il secondo profilo, quello dell'interazione con la rete, tra i principali temi da affrontare vi sono quello dell'età minima per l'accesso alle

non comporta il venir meno delle esenzioni dalla responsabilità stabilite nel presente regolamento, purché tali attività siano svolte in buona fede e in modo diligente […]".

151. Secondo cui "3. La motivazione di cui al paragrafo 1 contiene almeno le informazioni seguenti: […] c) ove opportuno, informazioni sugli strumenti automatizzati usati per adottare la decisione, ivi compresa l'informazione che indichi se la decisione sia stata adottata in merito a contenuti individuati o identificati per mezzo di strumenti automatizzati".

152. Tenuto conto che l'unico elemento fisico sul quale sarebbe possibile esercitare una forma di "dominio" sarebbe l'infrastruttura tecnica di rete, ove localizzata nei confini nazionali (cfr. Pollicino 2022, p. 338 ss.).

153. Si pensi ad Umberto Eco, secondo cui "I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel. È l'invasione degli imbecilli" (cfr. Nicoletti 2015).

154. Marchetti 2023, p. 471 ss.

155. Si vedano, in tal senso, i dati rilevati dall'OCSE e dalla *European Union Agency for Fundamental Rights* (FRA).

156. L'ammissibilità di limiti all'esercizio dei diritti, del resto, è espressamente riconosciuta da C. cost. 5 giugno 1956 n. 1, in *www.giurcost.org*, nonché da pronunce come Cass. pen. sez. I, 28 febbraio 2001, n. 341, in *Foro it.*, 2001, II, 457, secondo cui "il diritto alla libera manifestazione del pensiero, tutelato dall'art. 21 della Costituzione, non può essere esteso fino alla giustificazione di atti o comportamenti che, pur estrinsecandosi in una esternazione delle proprie convinzioni, ledano tuttavia altri principi di rilevanza costituzionale ed i valori tutelati dall'ordinamento giuridico interno e internazionale".

piattaforme (già introdotta – in Italia – per i siti pornografici[157] e in altri Paesi anche per i social[158]) e del superamento dell'anonimato, mediante forme di controllo effettivo dell'identità degli utenti[159].

6. Sesto potere e sovranità nelle "zone grigie"

La complessità del fenomeno in esame è evidente e pone interrogativi cui è difficile fornire adeguate risposte.

Non v'è dubbio che la libertà d'espressione, nella propria plurisecolare evoluzione[160], abbia preso le distanze dall'obbligo di dire la verità che gli antichi greci imponevano agli uomini liberi, quando prendevano la parola nelle assemblee pubbliche[161].

Tale evoluzione, se da un lato ha valorizzato (in chiave personalistica) il profilo di "libertà negativa"[162], così alimentando (anche indirettamente) il modello pluralistico-democratico, dall'altro, con l'avvento delle nuove tecnologie in ambito di comunicazione, sta determinando un concreto *vulnus* nella dimensione partecipativa alla sfera pubblica, che pure costituisce uno dei fondamentali obiettivi cui tendono le disposizioni contenute in Dichiarazioni, Convenzioni, Costituzioni e norme comunitarie/eurounitarie in materia, e che viene pregiudicata sia dalle fake news, poiché capaci di indurre valutazioni e decisioni errate (poiché fondate su presupposti non veritieri), sia dall'hate speech, che non costituisce "pensiero contrario" tutelato dalla libertà d'espressione, quanto piuttosto "pensiero antagonista" rispetto ai valori accolti dagli ordinamenti democratici e dalla Costituzione repubblicana[163].

Si sta assistendo, in proiezione antagonistica rispetto al "Quarto potere" della stampa[164] e al "Quinto potere" della radiotelevisione[165], alla

157. Di recente, il d.l. 15 settembre 2023, n. 123 (recante "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale.") ha previsto (cfr. art. 13 bis) forme di verifica della maggiore età per l'accesso a siti pornografici, ricollegando tale misura alla necessità di tutela dei minori, in chiave di "salute pubblica".

158. Come recentemente disposto in Australia (cfr. Franceschini 2024).

159. Tra le quali potrebbe aver senso anche l'utilizzo dello SPID o della CIE.

160. Segnata dal *Bill of Rights* inglese del 1689 (cit. "…the said Lords Spiritual and Temporal and Commons… declare… That the freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place out of Parliament"), dal sopra citato Primo Emendamento della Costituzione americana del 1789-1791, dalla Dichiarazione dei diritti dell'uomo e del Cittadino del 1789 (art. 11 – "La libera manifestazione dei pensieri e delle opinioni è uno dei diritti più preziosi dell'uomo; ogni cittadino può dunque parlare, scrivere, stampare liberamente, salvo a rispondere dell'abuso di questa libertà nei casi determinati dalla Legge"), dalla Dichiarazione Universale dei Diritti Umani proclamata dall'ONU nel 1948 (art. 19 – "Ogni individuo ha diritto alla libertà di opinione e di espressione incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere"), dalla Convenzione europea dei diritti dell'uomo del 1950 (art. 10 – "Hai il diritto di dire e di scrivere in modo responsabile quello che pensi e di comunicare e ricevere informazioni. Tale diritto include la libertà di stampa."), dalla Carta dei diritti fondamentali dell'Unione europea del 2000 (art. 11 – "1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. 2. La libertà dei media e il loro pluralismo sono rispettati.").

161. Cfr. Papa 2021-a, p. 56.

162. Garantendo uno spazio di tutela nei confronti dei pubblici poteri.

163. Sulla distinzione tra pensiero contrario e pensiero antagonista, cfr. Papa 2021-a, pp. 61-62.

164. Espressione coniata da Edmund Burke che, in un discorso alla Camera dei Comuni del Parlamento del 1787, ha così qualificato i media ed in particolare la stampa, in aggiunta ai tre poteri teorizzati da Montesquieu, come strumento indispensabile per la libertà e la democrazia, anche quale contrappeso agli altri poteri dell'ordinamento pubblico. In dottrina, si segnalano, Russ-Mohl 2015, p. 647 e Luzi 2014, p. 87 ss.

165. Il riferimento è al pluripremiato film di Sidney Lumet, *Quinto potere*, del 1976, sul mondo televisivo statunitense degli anni Settanta, anche se analogo titolo è stato adottato anche per il film di Bill Condon, *Il quinto potere*,

crescita di una sorta di "Sesto potere", che nasce direttamente in mano privata, si fonda sulle nuove tecnologie e sui c.d. Big Data e sfugge, almeno per ora, alle più attente discipline di stampo pubblicistico dei due tradizionali poteri sopra citati, volte a perseguire (non senza criticità, come detto) il pluralismo, la trasparenza e l'indipendenza dell'informazione.

Tale condizione è enfatizzata proprio dalle difficoltà di inquadramento giuridico delle piattaforme che, se da un lato rappresentano un innegabile spazio pubblico di confronto, dall'altro alimentano dinamiche non sempre sane, caratterizzate da una commistione tra interessi pubblici e interessi e decisioni – anche para-giurisdizionali – privati, che rischia di pregiudicare i diritti fondamentali degli utenti, attraverso forme di bilanciamento di dubbia trasparenza/indipendenza, ancorate ad attività di moderazione assimilate a vere e proprie forme di censura[166], rispetto alle quali i valori democratici sottesi alla libertà d'espressione appaiono talvolta recessivi rispetto a quelli economici, anche in dissonanza con l'ormai acquisita dimensione orizzontale delle disposizioni costituzionali[167].

Tali incertezze si riflettono anche sulle strategie di regolamentazione, passate dal modello privatistico delle *policies* contrattuali (termini di servizio), al c.d. *soft law* "partecipato" (codici di condotta) e, solo da ultimo, ad una regolamentazione di *hard law* (es. DSA), che se da un lato conferma come il dibattito sulla funzione *latu sensu* pubblicistica delle piattaforme sia ormai decisamente più maturo[168], dall'altro non risolve le incertezze di inquadramento, né rimarca in modo del tutto convincente il ruolo dei pubblici poteri nel bilanciamento di interessi delicati come quelli in esame.

Una volta esclusa, quindi, la possibilità di assimilare piattaforme e stampa o radiotelevisione, ma anche di esaminare il fenomeno con la sola lente privatistica, occorre riconoscere come gli ordinari confini tra diritto pubblico e privato siano ormai significativamente erosi[169], specie negli ambiti in cui interessi pubblici ed interessi tecnico-economici (e la digitalizzazione è uno di essi) tendono a sovrapporsi[170].

Nulla di nuovo, in realtà, ove si prenda in esame – senza pretesa di esaustività, ma alla luce della comune matrice europea – la controversa categoria degli "organismi di diritto pubblico": soggetti privati assoggettati all'osservanza delle procedure di aggiudicazione degli appalti pubblici[171], poiché istituiti per soddisfare esigenze di interesse generale, aventi carattere non industriale o commerciale, dotati di personalità giuridica, sottoposti ad influenza pubblica dominante.

È chiaro che tale fattispecie si riferisca ad altro rispetto alle piattaforme, ma è altrettanto vero come la sua gestazione testimoni – in modo analogo all'adozione del DSA – l'evidente tentativo del potere pubblico di riaffermare la propria sovranità[172] su quelle zone grigie che, altrimenti, sfuggirebbero al suo imperio, progressivamente assottigliato dalle dinamiche della globalizzazione e affiancato da nuovi poteri oligopolistici e talvolta

del 2013, su Julian Assange e WikiLeaks. In dottrina, si segnalano Baglioni 2009, p. 397 ss. e Berselli 2000, p. 154 ss.

166. Cfr. Monti 2019-a, p. 35 ss.

167. Teoria espressa dalla giurisprudenza costituzionale tedesca degli anni Cinquanta e poi fatta propria dalle principali corti costituzionali europee, dalla Corte europea dei diritti dell'uomo e dalla Corte di giustizia dell'Ue (come evidenziato da Pollicino 2019, p. 12 ss.). In merito si segnala la risalente, ma quasi predittiva, opera di Lombardi 1967, ove già si sosteneva l'importanza dell'applicazione dei diritti costituzionali anche nei rapporti tra privati.

168. Cfr. Sorice 2020, p. 371 ss.

169. Cfr. Cremona 2023, p. 179 ss.

170. Tali osservazioni, del resto, erano già presenti in Giannini 1995.

171. *Ex multis*, Monorchio–Mottura 2021, p. 14 ss.

172. Interessante, in tal senso, è la ricostruzione di Pelleriti 2021, p. 429 ss., che evidenzia come l'Ue, dinanzi ad una sorta di Corte Suprema di Facebook, del tutto slegata dagli ordinamenti giuridici cui gli utenti appartengono, con il DSA, stia certando di riaffermare il ruolo dei poteri pubblici e dei valori degli ordinamenti giuridici di appartenenza degli utenti delle piattaforme online. E, in termini ancor più chiari, Casolari 2024, p. 462 ss.

antagonisti[173] (assimilabili per certi versi agli "State actors" statunitensi[174]), che impongono un'attenta analisi e regolamentazione, passibile di incidere anche sull'esercizio della libertà d'espressione.

Non si trascurano, in queste riflessioni, i profondi e illuminanti pensieri di Mortati, Jemolo, Fois[175] che, difendendo l'interpretazione più ampia della libertà d'espressione, erano (e sono) di grande insegnamento, ma si osserva che i pericoli conseguenti alla compressione di tale diritto, dopo l'esperienza dei totalitarismi, non appaiono dissimili da quelli correlati ad una sua interpretazione anarchica, individualistica e de-funzionalizzata (nel mondo digitale), idonea a mettere a rischio proprio i valori democratici che dovrebbe preservare, e tutto ciò a beneficio di una libertà d'impresa degli operatori di mercato che si espande – pur ricollegandosi "storicamente" all'esercizio di un diritto condizionato – in modo quasi incontrollato (come ci ricordano le recenti scelte dei social, in ambito di fact-checking, dopo la recenti elezioni statunitensi[176]).

Ed ecco, quindi, che appare indispensabile valorizzare il fatto che, nei termini di cui al presente contributo, si parla di fake news e discorsi d'odio in rete, e che pertanto tali fattispecie vadano esaminate partendo dalle categorie generali, ma con la consapevolezza di necessari adeguamenti rispetto al "mondo digitale", che ormai rivendica un'autonoma dignità di inquadramento giuridico (se non addirittura ordinamentale[177]) e che giustifica anche bilanciamenti differenti e limitazioni che, nel "mondo analogico", sarebbero difficilmente accettabili. L'idea di un "marketplace of ideas"[178], secondo cui la massima circolazione dei contenuti su Internet sarebbe utile per consentire la formazione di opinioni libere da parte dei destinatari, ne risulterebbe rafforzata, in chiave virtuosa, in quanto permarrebbe l'accesso generalizzato ad informazioni pluralistiche, ma veritiere e non discriminatorie. D'altro canto, la più ampia libertà d'espressione cui siamo tradizionalmente abituati riprenderebbe ad espandersi lontano dai rischi (anche sistemici) della comunicazione on-line, prendendo atto delle utopie di Internet, dei mutamenti antropologici del XXI secolo e delle conseguenti implicazioni per le democrazie ed il diritto costituzionale[179].

L'approccio del DSA, rispetto a tali considerazioni, è evidentemente diverso[180]. Solo il tempo, vista la sua recente entrata in vigore e l'incognita della sua concreta implementazione[181], ci saprà dire se l'approccio scelto, più prudente, sia in grado di contrastare adeguatamente i fenomeni in esame, o se invece l'Ue e – nei limiti delle proprie

173. Ne è un esempio proprio lo scontro tra Donald Trump ed alcune piattaforme social, che in parte è diventato scontro tra la più importante democrazia occidentale e soggetti privati in essa stessa aventi sede.

174. Sul tema si segnala l'interessante ricostruzione di Niro 2023, p. 256 ss., che richiama il *leading case Marsh v. Alabama*, 326 U.S. 501 (1946), nonché il caso *Manhattan Community Access Corp. v. Halleck*, 587 U.S. (2019), secondo cui sono "State actors" i soggetti privati che esercitano "poteri tradizionalmente ed esclusivamente riservati allo Stato".

175. Tutti richiamati in Tanzarella 2023, p. 166 ss., cui si rinvia anche per la bibliografia.

176. Sul tema, *inter alia*: Isaac–Schleifer 2025; McMahon–Kleinman–Subramanian 2025; Rociola 2025.

177. Ed il pensiero va, inevitabilmente, al pensiero di Santi Romano, specie alla luce della creazione di corti supreme private che, come detto, ricalcano l'esercizio di poteri ordinamentali pubblicistici.

178. Teorizzata dal giudice Holmes nella *dissenting opinion* relativa alla decisione della Corte Suprema degli Stati Uniti *Schenk v. United States*, 249 U.S. 47 (1919).

179. Si vedano, in tal senso: Simoncini 2021, p. 723 ss., che evidenzia come il potere tecnologico imponga sfide completamente diverse rispetto a quelle affrontate nelle costituzioni ottocentesche (prima stagione) e post-belliche (seconda stagione), rimarcando il fondamentale – e crescente – ruolo delle autorità indipendenti; e ancora Longo 2023-a, p. 147 ss., ma anche Longo 2023-b, p. 103 ss., che giunge ad enunciare tre nuovi (meta) principi "di cui non potremo fare a meno": la "giustizia dei dati", la "trasparenza algoritmica" e il "controllo umano".

180. Come evidenziato, criticamente, anche da Giordano 2023, p. 193 ss., che solleva dubbi sulla portata innovativa del DSA rispetto alla c.d. direttiva "e-commerce".

181. Tema sul quale si rinvia a Sabia 2023, p. 88 ss., che si concentra sull'architettura multilivello dei poteri di enforcement.

competenze – i singoli Stati che la compongono, proseguendo quel lungo percorso iniziato con l'autoregolamentazione, e mutato dopo breve tempo, debbano adottare un approccio più radicale.

Quel che è certo è che la partita è tutta da giocare e che risultano ancora di enorme attualità le parole pronunciate – ormai oltre venticinque anni fa – da uno dei pionieri di Internet (Bill Gates), secondo cui "l'età dell'informazione che si è aperta offre possibilità immense di avviare nuove società e di fare grandi progressi… la rivoluzione delle comunicazioni è una ragione di forza, ma non è una panacea per tutti i mali. È importante anche discutere ampiamente tutte le implicazioni, buone e cattive, del progresso tecnologico, in modo che sia la società e non i tecnocrati a guidarci in questo viaggio"[182].

Riferimenti bibliografici

Aa.Vv. (2023), *Il* Digital Services Act *e il contrasto alla disinformazione: responsabilità dei* provider*, obblighi di* compliance *e modelli di* enforcement, in "MediaLaws", 2023, n. 2

F. Abbondante (2017), *Il ruolo dei social network nella lotta all'*hate speech*: un'analisi comparata fra l'esperienza statunitense e quella europea*, in "Informatica e diritto", 2017, n. 1-2

L. Albertini (2020), *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione sul ruolo dei gatekeepers della comunicazione)*, in "MediaLaws", 2020, n. 4

M.R. Allegri (2018), *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2018

L. Aria (2021), *L'attività delle piattaforme tra DSA e Direttiva SMAV. La frontiera di una nuova regolazione?*, in "MediaLaws", 29 gennaio 2021

C. Asprella (2023), *L'Oversight Board, la "Corte d'appello" di Facebook, e i nuovi "confini" della giurisdizione*, in "Judicium", 2023, n. 3

A. Baglioni (2009), *È nato il "quinto potere"? L'opinion making. Giuliano Ferrara e Vittorio Feltri*, in "Problemi dell'informazione", 2009, n. 4

M. Bassini (2019), *Internet e libertà d'espressione. Prospettive costituzionali e sovranazionali*, Aracne, 2019

E. Berselli (2000), *Il giornalismo alla svolta digitale. Quarto potere, addio. Politica in crisi nell'e-world, ma il giornalismo non la sa raccontare*, in "Problemi dell'informazione", 2000, n. 2

E. Bertolini (2021), *Alternative Facts, Political Lies and Freedom of Expression: A Paradigm of Trump's Administration*, in "DPCE online", 2021, n. 1

M. Betzu (2022), *Libertà senza responsabilità? La Corte Edu e l'anonimato "online"*, in "Quaderni costituzionali", 2022, n. 2

M. Betzu (2011), *Anonimato e responsabilità in internet*, in "Costituzionalismo.it", 2011, n. 2

E. Birritteri (2023), *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in "MediaLaws", 2023, n. 2

L. Bolognini, E. Pelino, M. Scialdone (a cura di) (2023), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè, 2023

P. Bonini (2020), *L'autoregolamentazione dei principali "Social Network". Una prima ricognizione delle regole sui contenuti politici*, in "federalismi.it", 2020, n. 11

182. Gates 1997, p. 404.

R. Borrello (2023), *Vecchi e nuovi limiti della libertà d'espressione*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

M.E. Bucalo (2023) *La libertà di espressione nell'era dei* social network *fra* content moderation *e necessità di una regolazione flessibile*, in "Diritto pubblico comparato ed europeo", 2023, n. 1

M.E. Bucalo (2022), *La libertà di espressione in rete fra* content moderation *dei* social network *e regolazione dell'Unione Europea*, in "dirittifondamentali.it", 2022, n. 3

A. Buratti (2022), *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in "MediaLaws", 2022, n. 2

A. Candido (2020), *Libertà di informazione e democrazia ai tempi delle* fake news, in "federalismi.it", 2020, n. 20

G. Cané (2023), *Dopo Musk anche Zuckerberg riceve l'avviso della Ue: «Con i fatti di Israele, più attenzione contro le fake news»*, in "Corriere della Sera", 11 ottobre 2023

A. Canepa (2023), *La nozione di piattaforma e la disciplina applicabile*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

P. Caretti, A. Cardone (2019), *Diritto dell'informazione e della comunicazione nell'era della convergenza*, il Mulino, 2019

C. Caruso (2020), *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei* social network, in "Consulta Online", 17 marzo 2020

F. Casarosa (2020), *L'approccio normativo europeo verso il discorso dell'odio online: l'equilibrio tra un sistema di "enforcement" efficiente ed efficace e la tutela della libertà di espressione*, in "questionegiustizia.it", 8 luglio 2020

F. Casolari (2024), *Il* Digital Services Act *e la costituzionalizzazione dello spazio digitale europeo*, in "Giurisprudenza italiana", 2024, n. 2

G. Cerrina Feroni (2021), *Libertà di espressione, Garante privacy: "Troppo potere alle big tech, ecco come intervenire"*, 11 maggio 2021

C. Cipolloni (2023), *Il diritto all'anonimato: analisi dell'istituto e della sua evoluzione nell'età della rivoluzione internettiana*, in "dirittifondamentali.it", 2023, n. 3

A.M. Colman (2015), *A Dictionary of Psychology*, Oxford University Press, 2015

C.R. Combei (2023), *Social network: tra diritto di parola e necessità di regole*, in "www.treccani.it", 14 novembre 2023

Commissione europea (2022), *Firmatari del codice rafforzato di buone pratiche sulla disinformazione 2022*, 16 giugno 2022

Commissione Nazionale Italiana per l'UNESCO (2022), *È online il rapporto dell'UNESCO sulla libertà di espressione e lo sviluppo dei media*, 25 luglio 2022

E. Cremona (2023), *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Edizioni Scientifiche Italiane, 2023

M. Cuniberti (2022), *La professione del giornalista*, in G.E. Vigevani, O. Pollicino, C. Melzi D'Eril et al., "Diritto dell'informazione e dei media", Giappichelli, 2022

L. D'Agostino (2023), *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act, in "MediaLaws", 2023, n. 2

A. Davola (2022), *Nuove tecnologie e regolamentazione digitale*, in E. Battelli (a cura di), "Diritto privato digitale", Giappichelli, 2022

G. D'Ippolito (2021), *Profilazione e pubblicità targettizzata online.* Real-time Bidding *e* behavioural advertising, Edizioni Scientifiche Italiane, 2021

S. Del Gatto (2023), *Il* Digital Services Act*: un'introduzione*, in "Giornale di diritto amministrativo", 2023, n. 6

F. Di Ciommo (2003), *Internet e crisi del diritto privato: tra globalizzazione, dematerializzazione e anonimato virtuale*, in "Rivista critica del diritto privato", 2003, n. 1

A. Di Corinto (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Di Gregorio (2019), *La Russia e le elezioni europee*, in "federalismi.it", 2019, n. 11

F. Di Tano, R. Brighi (2019), *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche*, in "Rivista di filosofia del diritto", 2019, n. 1

L. Diotallevi (2015), *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"?*, in "Giurisprudenza costituzionale", 2015, n. 3

European Commission (2024), *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram*, 16 May 2024

G. Finocchiaro (2023), *Responsabilità delle piattaforme e tutela dei consumatori*, in "Giornale di diritto amministrativo", 2023, n. 6

G. Finocchiaro (2021), *Digital Service Act: la ridefinizione della limitata responsabilità del provider e il ruolo dell'anonimato*, in "MediaLaws", 12 gennaio 2021

S. Flaminio (2022), *Lotta alle "fake news": dallo stato dell'arte a una prospettiva di regolamentazione per il vivere digitale a margine del "Digital Services Act"*, in "Rivista italiana di informatica e diritto", 2022, n. 2

G.M. Flick, C. Flick (2022), L'*algoritmo d'oro e la torre di Babele*, Baldini+Castoldi, 2022

L. Flore (2023), *Disciplina dell'editoria e ordine dei giornalisti*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

E. Franceschini (2024), *Australia, social vietati ai minori di 16 anni: "Così li proteggiamo"*, in "La Repubblica", 29 novembre 2024

T.E. Frosini (2020), *Il Costituzionalismo nella Società tecnologica*, in "Consulta Online", 25 maggio 2020

A.E. Galeotti (2021), *Political Disinformation and Voting Behavior: Fake News and Motivated Reasoning*, in "Notizie di Politeia", 2021, n. 142

B. Gates (1997), *La strada che porta a domani*, Mondadori, 1997

M.S. Giannini (1995), *Diritto pubblico dell'economia*, il Mulino, 1995

F. Giglioni (2023), *Il servizio pubblico radiotelevisivo*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

G. Giordano (2023), *La responsabilità degli intermediari digitali nell'architettura del* Digital Services Act*: è necessario che tutto cambi affinché tutto rimanga com'è?*, in "Comparazione e diritto civile", 2023, n. 1

A. Granelli (2008), voce *Digital divide*, in Treccani, Enciclopedia della Scienza e della Tecnica, 2008

O. Grandinetti (2021), Facebook vs. CasaPound e Forza Nuova*, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in "MediaLaws", 2021, n. 1

T. Groppi, A. Simoncini (2012), *Introduzione allo studio del diritto pubblico e delle sue fonti*, Giappichelli, 2012

A. Iannotti della Valle (2021), *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il "modello" dell'*Oversight Board *di Facebook*, in "federalismi.it", 2021, n. 26

D. Imbruglia (2022), *La responsabilità degli intermediari*, in E. Battelli (a cura di), "Diritto privato digitale", Giappichelli, 2022

V. Iorio (2024), *Battaglia tra Ue e Musk: "Il suo X viola le regole". Lui: vogliono la censura*, in "Corriere della sera", 13 luglio 2024

M. Isaac, T. Schleifer (2025), *Meta Says It Will End Its Fact-Checking Program on Social Media Posts*, in "The New York Times", 7 gennaio 2025

P. Kowalicka (2022), *La politica digitale dell'unione europea*, in G. Ziccardi, P. Pierri (a cura di), "Competenze digitali per il giurista", Giuffrè, 2022

A. Lamberti (2023), *Libertà di informazione, poteri privati e tutela dei dati personali nell'era digitale*, in "dirittifondamentali.it", 2023, n. 3

G. Lombardi (1967), *Potere privato e diritti fondamentali*, Giappichelli, 1967

E. Longo (2023), *Libertà di informazione e lotta alla disinformazione nel* Digital Services Act, in "Giornale di diritto amministrativo", 2023, n. 6

E. Longo (2023-a), *La ricerca di un'antropologia costituzionale della società digitale*, in Rivista italiana di informatica e diritto, 2023, n. 2

E. Longo (2023-b), *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in "Diritto pubblico comparato ed europeo", 2023, n. 1

N. Lucchi (2011), *Internet, manifestazione del pensiero e responsabilità editoriale*, in "Quaderni costituzionali", 2011

M. Luzi (2014), *Quarto potere e massa nella società contemporanea*, in "Rivista trimestrale di scienza dell'amministrazione", 2014, n. 3

M. Manetti (2021), *Facebook, Trump e la fedeltà alla Costituzione*, in "Forum di quaderni costituzionali", 2021, n. 1

M. Manetti (2014), *Libertà di pensiero e anonimato in rete*, in "Il diritto dell'informazione e dell'informatica", 2014, n. 2

G. Marchetti (2023), *Le* fake news *e il rafforzamento degli strumenti per contrastarne la diffusione*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

G. Marchetti (2020), *Le* fake news *e il ruolo degli algoritmi*, in "MediaLaws", 2020, n. 1

S. Martinelli (2022), *Il giurista e la comprensione delle piattaforme*, in G. Ziccardi, P. Pierri (a cura di), "Competenze digitali per il giurista", Giuffrè, 2022

T. Martines (2000), *Diritto costituzionale*, Giuffrè, 2000

L. Mcmahon, Z. Kleinman, C. Subramanian (2025), *Facebook and Instagram get rid of fact checkers*, in "bbc.com", 7 January 2025

D. Messina (2021), *Televisione e servizi media audiovisivi*, in A. Papa, "Il diritto dell'informazione e della comunicazione nell'era digitale", Giappichelli, 2021

M. Mezzanotte (2018), Fake news *nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?*, in "federalismi.it", 2018, n. 24

A. Michinelli (2023), *L'interazione del DSA con altre regole sui servizi digitali*, in L. Bolognini, E. Pelino, M. Scialdone (a cura di), "Digital Services Act e Digital Markets Act", Giuffrè, 2023

M. Molinari (2019), *Populismo – Democrazia*, in "Gnosis", 2019, n. 4

A. Monorchio, L. Mottura (2021), *Compendio di contabilità di Stato*, Cacucci, 2021

M. Monti (2022), *Circolazione dei contenuti:* fake news *e* hate speech *fra UE e Stati Uniti*, in E. Battelli (a cura di), "Diritto privato digitale", Giappichelli, 2022

M. Monti (2022-a), *Lo strengthened Code of Practice on Disinformation: un'altra pietra della nuova fortezza digitale europea?*, in "MediaLaws", 2022, n. 2

M. Monti (2021), *La Corte Suprema statunitense e il potere delle piattaforme digitali: considerazioni sulla privatizzazione della censura a partire da una concurring opinion*, in "DPCE online", 2021, n. 1

M. Monti (2020), *La disinformazione "online", la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in "federalismi.it", 2020, n. 11

M. Monti (2019), *Il* Code of Practice on Disinformation *dell'UE: tentativi* in fieri *di contrasto alle* fake news, in "MediaLaws", 2019, n. 1

M. Monti (2019-a), *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in "Rivista italiana di informatica e diritto", 2019, n. 1

L. Musselli (2023), *La disciplina dell'audiovisivo in Italia*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

A. Napolitano (2021), *La libertà di informazione professionale*, in A. Papa, "Il diritto dell'informazione e della comunicazione nell'era digitale", Giappichelli, 2021

A. Nicastro (2023), *Informazione e misinformazione: cosa ci insegna la guerra in Ucraina*, Ordine dei Giornalisti Lombardia, 9 giugno 2023

L. Nicolao (2023), *Twitter, come funzioneranno gli account verificati dal 20 aprile. Musk: «Via le spunte blu a chi non paga»*, in "Corriere della sera", 23 aprile 2023

G. Nicoletti (2015), *Umberto Eco: "Con i social parola a legioni di imbecilli"*, in "La Stampa", 11 giugno 2015

R. Niro (2023), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolamentazione: note ricostruttive*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

R. Niro (2021), *Piattaforme digitali e libertà d'espressione fra autoregolamentazione e coregolamentazione: note ricostruttive*, in "Osservatoriosullefonti.it", 2021, n. 3

G. Pagano (2019), *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in "federalismi.it", 2019, n. 11

E. Palici di Suni (2020), Fake news *e referendum*, in "federalismi.it", 2020, n. 11

A. Palumbo, J. Piemonte (2023), *Delega di funzioni regolamentari e lotta ai rischi sistemici causati della disinformazione nel* Digital Services Act*: quali rischi per la libertà di espressione?*, in "MediaLaws", 2023, n. 3

A. Papa (2021), *Il diritto dell'informazione e della comunicazione nell'era digitale*, Giappichelli, 2021

A. Papa (2021-a), *La libertà di manifestazione del pensiero*, in Id., "Il diritto dell'informazione e della comunicazione nell'era digitale", Torino, 2021

M. Pedretti (2023), *X finisce nel mirino della Commissione Europea*, in "PC professionale", 18 Dicembre 2023

C. Pedullà (2018), *L'amministratore di un sito internet non è responsabile ai sensi dell'art. 57 c.p.*, in "Cassazione penale", 2018, n. 11

E. Pelino (2023), *Esenzione di responsabilità, libero pensiero e manipolazione dei contenuti*, in L. Bolognini, E. Pelino, M. Scialdone (a cura di), "Digital Services Act e Digital Markets Act", Giuffrè, 2023

S. Pelleriti (2021), *La* governance *privata di Facebook e la presa di coscienza del regolatore europeo: qualcosa sta cambiando?*, in "Rivista della regolazione dei mercati", 2021, n. 2

G. Pistorio (2023), *Libertà di espressione e di informazione*, in "Rapporto sullo stato dei diritti in Italia", 15 dicembre 2023

G. Pitruzzella (2018), *La libertà di informazione nell'era di Internet*, in "MediaLaws", 2018, n. 1

O. Pollicino (2022), *Ruoli e responsabilità in rete*, in G.E. Vigevani, O. Pollicino, C. Melzi D'Eril et al., "Diritto dell'informazione e dei media", Giappichelli, 2022

O. Pollicino (2019), *L'"autunno caldo" della Corte di giustizia: diritti fondamentali in rete e sfide del costituzionalismo alle prese con i poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19

O. Pollicino (2018), *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in "MediaLaws", 2018, n. 1

O. Pollicino, P. Dunn (2024), *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in "federalismi.it", 2024, n. 12

F. Posteraro (2020), *Piattaforme digitali sono come editori ma senza responsabilità editoriale, basta immunità*, in "il Riformista", 2 giugno 2020

A. Punzi (2024), *Governance condivisa: la regolazione dei contenuti in rete oltre la separazione tra pubblico e privato*, in "Giurisprudenza italiana", 2024, n. 2

E.C. Raffiotta (2023), *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in "Osservatorio sulle fonti", 2023, n. 2

G.M. Riccio (2000), *Anonimato e responsabilità in Internet*, in "Il diritto dell'informazione e dell'informatica", 2000, n. 2

A. Rociola (2025), *Facebook cancella il fact-checking: basta censura*, in "La Stampa", 8 gennaio 2025

S. Rodotà (2014), *Recensione* a G. De Minico, Internet. Regola e anarchia, Napoli, Jovene, 2012, in "Diritto pubblico", 2014, n. 1

U. Ruffolo (2024), *Piattaforme e* content moderation *negoziale*, in "Giurisprudenza italiana", 2024, n. 2

S. Russ-Mohl (2015), *Gli impotenti eroi del quarto potere*, in "Problemi dell'informazione", 2015, n. 3

R. Sabia (2023), *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in "MediaLaws", 2023, n. 2

K.W. Saunders (1996), *Violence as Obscenity: Limiting the Media's First Amendment Protection*, Duke University Press, 1996

L. Scaffardi (2009), *Oltre i confini della libertà d'espressione. L'istigazione all'odio razziale*, CEDAM, 2009

G. Scorza (2023), *La lezione di Cambridge Analytica: leggere prima di accettare, per sopravvivere nell'universo digitale*, in "huffingtonpost.it", 6 giugno 2023

V. Sellaroli (2019), *Presupposti e criteri di imputabilità del blogger per commenti diffamatori postati dagli utenti*, in "ilPenalista.it", 13 maggio 2019

G. Sgueo (2023), *L'architettura istituzionale del* Digital Services Act, in "Giornale di diritto amministrativo", 2023, n. 6

A. Simoncini (2022), *La co-regolazione delle piattaforme digitali*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di Stato e forma di governo*, in "Osservatoriosullefonti.it", 2021, n. 2

M. Sorice (2020), *La 'piattaformizzazione' della sfera pubblica*, in "Comunicazione politica", 2020, n. 3

A. Stiano (2022), *Facebook e diritto alla libertà di espressione: il "caso Trump" tra istanze personalistiche, auto regolamentazione e diritto internazionale*, in "Rassegna di diritto civile", 2022, n. 3

P. Tanzarella (2023), *I discorsi d'odio*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), "Informazione e media nell'era digitale", Giuffrè, 2023

A. Titterington (2023), *Allerta truffatori con i segni di spunta blu su Twitter X*, in "kaspersky daily", 23 ottobre 2023

L. Tormen (2019), *La linea dura della Cassazione in materia di responsabilità dell'*hosting provider *(attivo e passivo)*, in "La nuova giurisprudenza civile commentata", 2019, n. 5

G. Vasino (2023), *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in "federalismi.it", 2023, n. 4

G.E. Vigevani (2023), *Dal "caso Casapound" del 2019 alla "sentenza Casapound" del 2022: piattaforme digitali, libertà d'espressione e odio on line nella giurisprudenza italiana*, in "MediaLaws", 2023, n. 2

G.E. Vigevani (2021), *Articolo 21*, in F. Clementi, L. Cuocolo, F. Rosa, G.E. Vigevani (a cura di), "La Costituzione italiana. Commento articolo per articolo", il Mulino, vol. I, 2021

G.E. Vigevani (2014), *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in "Il diritto dell'informazione e dell'informatica", 2014, n. 2

A. Vigorito (2020), *Piattaforme digitali e "political speech": dal caso Facebook-CasaPound alla vicenda Twitter-Trump*, in "giustiziacivile.com", 2020, n. 11

S. Vimercati (2021), *La responsabilità del gestore del sito per i contenuti pubblicati da soggetti terzi*, in "MediaLaws", 2021, n. 2

S. Vimercati (2018), *Il revirement della Cassazione: la responsabilità per omesso controllo si applica al direttore della testata telematica*, in "MediaLaws", 2018, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0222 • articolo sottoposto a peer review • pubblicato in anteprima il 4 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

CHRISTIANE MAAß – CHIARA FIORAVANTI

Evaluating the performance of DeepL as translation tool between German and Italian Easy Language administrative texts

Easy Language (EL), a comprehensibility-optimised form of a natural language that makes content accessible to people with communication impairments, can play an important role in institutional communication. However, the extent to which it is adopted for legal and administrative texts has not progressed evenly in the various countries. Interlingual translation could be an asset to increase the use of EL in this domain, also considering that recently AI-driven tools have become an important support for translation. The project that will be presented aims to evaluate the possibility of using DeepL as an automated translation tool for interlingual translation into EL particularly in the domain of administrative texts. To this end, the performance of DeepL was analysed for the language pair German and Italian, using a EL bilingual corpus produced by the administration of the Province of Bolzano/Bolzen. The machine-generated corpus texts were evaluated for readability, correctness and compliance with the EL rules and compared with the gold standard texts, in order to identify the potentials and limitations of the translation and the possible need for post-editing.

Administrative texts – Easy Language – Leichte Sprache – Lingua facile – AI translation tools
Accessible Communication

Valutazione delle prestazioni di DeepL come strumento di traduzione tra testi amministrativi tedeschi e italiani in Lingua facile

L'Easy Language (EL), forma di linguaggio naturale ottimizzata per la comprensibilità da parte delle persone con difficoltà di comunicazione, può svolgere un ruolo importante nella comunicazione istituzionale. Tuttavia, l'adozione di questa modalità comunicativa in ambito giuridico-amministrativo non è uniforme in Paesi diversi. La traduzione interlinguistica può rappresentare un'opportunità per aumentare l'uso dell'EL in questo settore, anche considerando che recentemente gli strumenti di traduzione IA sono diventati un importante supporto. Lo studio qui presentato mira a valutare la possibilità di utilizzare DeepL come strumento di traduzione automatica per la traduzione interlinguistica in EL, in particolare nel campo dei testi amministrativi. A tal fine, sono state analizzate le prestazioni di DeepL per le lingue tedesca e italiana usando un corpus derivato da testi in EL prodotti nelle due lingue dall'amministrazione della Provincia di Bolzano. I testi del corpus generati dalla macchina sono stati valutati per leggibilità, correttezza e conformità alle regole dell'EL e confrontati con i testi "gold standard", al fine di individuare le potenzialità e i limiti della traduzione e l'eventuale necessità di post-editing.

Testi amministrativi – Easy Language – Leichte Sprache – Lingua facile – Strumenti IA di traduzione
Comunicazione accessibile

C. Maaß is Professor for Media Linguistics, Institute for Translatology and Specialised Communication at the University of Hildesheim (Germany) and Director of the Research Centre for Easy Language (Forschungsstelle Leichte Sprache). C. Fioravanti is a researcher at the Institute of Legal Informatics and Judicial Systems of the National Research Council of Italy

Summary: 1. Introduction. – 2. Previous Research. – 2.1. Guidelines for Easy Language in Italian and German. – 2.2. Easy Language for legal and administrative texts in Germany and Italy. – 2.3. Research on AI tools for Easy Language Translation. – 3. Research Design. – 3.1. Corpus source. – 3.2. Corpus characteristics. – 3.3. Procedure of analysis. – 4. Results. – 4.1. Readability scores. – 4.2. Correctness. – 4.3. Deviation from the German/Italian Easy Language guidelines. – 5. Summary and Discussion.

1. Introduction

Easy Language (in German: *Leichte Sprache*; in Italian: *Lingua facile*) is a comprehensibility-optimised form of a natural language that makes content accessible to people with communication impairments, including cognitive impairments[1]. Easy Language is part of international regulatory efforts aimed at enabling greater participation and communicative inclusion. In recent years, developments in this area have not progressed evenly in the various countries. Some countries already have regulations, scientific foundations and extensive textual practice, while others still have a long way to go[2]. The professional and financial resources available for Easy Language texts in the various countries and for various natural languages are also very different.

Recently, AI-driven tools have become an increasingly important part of translation work in Easy Language translation[3]. They can be used for intralingual and interlingual translation[4].

This paper analyses the performance of DeepL for interlingual translation between German and Italian Easy Language administrative texts.

DeepL is a powerful translation tool that has found its way into interlingual translation in recent years and has contributed to significant increases in productivity. If DeepL could be used to produce correct and sufficiently easy target texts in many languages, then existing resources from different countries could be better exploited and a much larger number of texts could be produced with limited resources. This method could also be used to create texts for people with different first languages in one country (e.g., for recent migrants in a host society[5]) or to create an additional English-language offer in Easy Language[6].

This article therefore evaluates the possibility of using DeepL as a machine translation tool for interlingual translation[7] into Easy Language in the administrative information domain.

1. Maaß 2015; Bredel–Maaß 2016-a; Maaß 2020; Maaß 2024-a.
2. See the contributions in Lindholm–Vanhatalo 2021 on the situation of Easy Language in 20 different European countries.
3. Deilen–Hernández Garrido–Lapshinova-Koltunski–Maaß 2023, Deilen–Lapshinova-Koltunski–Hernández Garrido 2024; Kopp–Rempel–Schmidt–Spiess 2023; Spring–Kostrzewa–Fröhlich 2023.
4. Maaß 2024-a, Maaß 2024-b.
5. For reflections on Easy Language texts for migrants with low second language skills see Ahrens–Fioravanti 2022.
6. For a first exploration see Kaplan 2021.
7. Easy Language currently belongs predominantly to the domain of intralingual translation. The use of AI tools for intralingual translation has already been tested in this field (see Deilen–Hernández Garrido–Lapshinova-Koltunski–Maaß 2023, Deilen–Lapshinova-Koltunski– Hernández Garrido 2024: they stress the role of post-editing in the process).

For the present study, texts from an interlingual German/Italian translation project were taken as the starting point for the analysis. The gold standard texts are texts from the administrative communication of the municipality of Bolzano, which were drafted in German Easy Language and were then translated by human translators into Italian Easy Language (interlingual translation). Both versions were drafted on the basis of the ruleset of the Research Centre for Easy Language (University of Hildesheim). Machine translations from both languages were then produced using DeepL and analysed for this article. The aim was to determine the performance of DeepL on various parameters with respect to readability, correctness and adherence to the Easy Language rulesets, as well as a possible need for post-editing. The German-Italian Easy Language project corpus is medium size for qualitative research. It is unique at the moment both in size and in quality.

2. Previous Research

2.1. Guidelines for Easy Language in Italian and German

The first reference guidelines for Italian and German Easy Language were created by the European Pathways project, carried out by the Inclusion Europe association. The project promoted European standards on how to make information easy to read and understand for many different European languages[8]. The Anffas national association was in charge of translating these standards into Italian. This activity also involved the participation of the end users with whom the translation was evaluated. Participation in the project enabled Anffas to give visibility to Easy Italian for the first time[9].

The Inclusion Europe regulations are also available for German, but they are not the most widely used practical ruleset in Germany: this role belongs to the ruleset of the Network Easy Language (*Netzwerk Leichte Sprache*). The Network Easy Language was founded in 2006 and presented its ruleset in 2011[10]. The third source of practical rules is the annex to the *Barrierefreie-Informationstechnik-Verordnung 2.0* (Accessible Information Technology Regulation 2.0) from 2011, which is part of public tenders and provides a list of central Easy Language rules[11].

Maaß[12] compares these three sets of rules, evaluates them and proposes modifications, taking into account the findings of comprehensibility research. Bredel and Maaß[13] broaden the scientific basis and contribute findings from various disciplines to the discourse on German Easy Language, paying particular attention to previous research on comprehensibility, reading acquisition, reading restrictions in various forms of disability, specialised communication, translation, xenolects and language varieties, all of which contribute to understanding what Easy Language should accomplish and how the texts must be structured in order to achieve this goal[14].

Based on the observation that the Inclusion Europe guidelines were too general and not specific to the Italian language, Sciumbata[15] has recently presented scientifically based Easy Language rules for Italian, drawing on international Easy Language research, comprehensibility research and research on the grammar and linguistic system of the Italian language. The new guidelines also include a review of existing guidelines for other languages and a thorough text analysis using quantitative and qualitative methods on an Italian corpus. They also incorporate evidence from studies on reading difficulties, as well as guidance already available from the literature on plain language and the simplification of legal and administrative language. Compared to their predecessors, the new guidelines focus more on linguistic and textual aspects and

8. Bredel–Maaß 2016-a; Maaß 2020.
9. Perego 2021.
10. Bredel–Maaß 2016-a; Bredel–Maaß 2016-b; Maaß 2020.
11. *Ibidem*.
12. Maaß 2015.
13. Bredel–Maaß 2016-a; Bredel–Maaß 2016-b.
14. English summary in Maaß 2020.
15. Sciumbata 2022.

also include suggestions on visualisations and on web content.

2.2. Easy Language for legal and administrative texts in Germany and Italy

Language in a legal and administrative context was the first domain in which Easy Language was legally recognised in Germany: since 2011, federal authorities have been required to provide Easy Language content on their websites[16]. In the following years, the obligation was extended to ever larger circles and more and more domains. Easy Language is now much more widespread in everyday life in Germany than it was just a few years ago, for example in health communication[17], in the news, but also in political discourse as part of participatory efforts[18], including in oral form as Easy Language interpreting[19]. Nevertheless, there are still major deficits with regard to the availability of Easy Language texts for various domains. The quality of Easy Language texts is also heterogeneous[20]. Producing Easy Language texts requires large resources that are not available everywhere to the necessary extent. The question of how to make comprehensive text offerings possible with limited resources is therefore virulent.

The simplification of legal and administrative language has been an issue of interest in Italy since the 1990s, but despite the many initiatives that have been taken in this direction over the years, both in the academic and research world and by the institutions themselves, it is as yet a persistent problem[21]. Italian institutional communication is still difficult for lay people, and therefore even less suitable for people with special communication needs. Easy Language in Italy had a precursor in the controlled writing techniques proposed by Piemontese[22]and applied to the magazine "Due Parole. Mensile di facile lettura", created in the 1980s at the University of La Sapienza[23]. In spite of this experience, Easy Language is still not very widespread. Italy lags far behind other countries in terms of Easy Language use and dissemination, although recently interest in the topic has gained traction especially at research level also thanks to participation in European projects[24].

On a practical side, one of the main producers of text in Italian Easy Language is Anffas, a national association of families of people with Intellectual disabilities, which has created several simplified documents, including many on legal issues[25]. For example, its website[26]currently contains information on the UN Convention on the Rights of Persons with Disabilities, the UN Convention on Children's Rights, the right to vote and the legal process of the referendum.

Germany is in a much more favourable position than Italy when it comes to implementing Easy Language text practices[27]. Hence, it is no coincidence that in Italy, the most virtuous public body in terms of this language policy is the Autonomous Province of Bolzano/Bozen, which has always looked to the German speaking area when planning its communication strategies. Here, following the German model, the provincial government passed a law in 2015 entitled "Participation and integration of people with disabilities", which has also been translated into Easy language[28]. Later on, the Province of Bolzano created a special section on its institutional website dedicated to in-

16. Rink 2020; Lang 2019, Lang 2021, Lang 2024; Maaß 2020.
17. Ahrens–Maaß 2024; Ahrens 2024; Kröger–Maaß 2024.
18. Maaß et al. 2021; Maaß–Schwengber 2022.
19. Schulz et al. 2020; Maaß–Maaß LM 2024.
20. Lang 2021; Maaß LM 2023.
21. Cortelazzo 2021.
22. Piemontese 1996.
23. Sciumbata 2021.
24. Perego 2021.
25. Sciumbata 2021.
26. See Anffas website.
27. Maaß et al. 2021.
28. Magris 2022; Sciumbata 2022.

formation in *Lingua facile* in Italian and German, which contains a plethora of information on different sectors, from which the corpus for this research was derived (see paragraph 3.1).

Legal and administrative texts are a challenge for translation into Easy Language because they contain a particularly large number of barriers that make the content difficult to access[29]. They are characterised by domain-specific terminology and syntax, they require familiarity with legal and administrative procedures and the facts presented are often complex in themselves because explicit or implicit references are made to laws and regulations. The effects of not understanding or misunderstanding are also often to the detriment of the user, because successful interaction with the administration is not possible if the authorities do not provide comprehensible communication. It therefore makes sense to transfer an existing best practice interlingually. This is what was done in the Province of Bolzano/Bozen, where legal and administrative texts were translated intralingually into Easy German and then interlingually into Easy Italian.

2.3. Research on AI tools for Easy Language Translation

AI tools have rapidly gained functionality for translation in recent years – both interlingually and intralingually. Intralingual translation into Easy Language is part of the concept of text simplification[30]. For German, both general chat-based tools such as Chat GPT and tools specifically designed for intralingual translation in German such as SUMM AI or FCSP are available[31]. For Italian, the authors are not aware of any tools specifically designed for intralingual Easy Language translation. General tools such as Chat GPT work for various individual languages, although their performance is likely to depend on the extent to which the tool has been trained and the amount of data used. For German, Deilen et al.[32] have presented a first study on the performance of Chat GPT as a tool for intralingual Easy Language translation. To our knowledge, no studies on Italian Easy Language or comparative language studies with respect to different Easy Languages for this type of machine have been published to date. However, research on automatic text simplification (ATS) has been highly active in recent years. Notable contributions comprise the research of Ryan et al.[33], which released a multilingual text simplification benchmark that covers Italian language; the first in-depth investigation of LLMs' capabilities for ATS in Italian by Nozza and Attanasio[34]; Miliani et al.[35] study on the simplification of Italian administrative texts for L2 readers; and Russodivito et al.[36]research on the effectiveness of LLMs in simplifying Italian administrative texts compared to human-based simplification.

AI-generated interlingual translation tools have significantly changed the translation market in recent years. DeepL is one of the AI-driven translation engines that is available to a wide audience and offers very high performance. In the study by Fitria[37], texts translated with DeepL contained less than half as many issues as those translated with Microsoft Translator and Google Translate. Kaplan[38] examines the use of various machine translation engines for the production of accessible texts, especially for administrative texts, focussing on the French-English language pair. She shows that easy-to-read texts have specific problems in interlingual translation, some of which can be solved by pre- and post-editing procedures.

29. Rink 2020, Rink 2024; Maaß 2024-a.
30. Štajner et al. 2018; Kopp–Rempel–Schmidt–Spiess 2023.
31. Deilen et al. 2023, Deilen et al. 2024; see Hansen-Schirra et al. 2020 for technological solutions in Easy Language translation in more general terms.
32. Deilen et al. 2023.
33. Ryan et al. 2023.
34. Nozza–Attanasio 2023.
35. Miliani et al. 2023.
36. Russodivito et al. 2024.
37. Fitria 2023.
38. Kaplan 2021.

However, there have not yet been any systematic studies on interlingual translation into Easy Language using DeepL as a machine translation tool for the language pair German-Italian.

Just a few years ago, Wiesmann[39] was sceptical about the use of neural machine tools in Italian/German legal translation: she found that the target texts contained too many errors to make further processing via post-editing appear worthwhile. However, this situation has now changed and AI tools are now part of translation practice in the field of specialised communication. The desiderata described in Maaß et al.[40], namely that no CAT tools or machine translation tools are available for Easy Language, are thus at least partially fulfilled. Deilen et al.[41] show that post-editing remains a necessary part of intralingual translation. This is in line with the results for interlingual translation[42].

3. Research Design

3.1. Corpus source

The performance analysis of DeepL relies on a corpus extracted from the section of the website of the Administration of the Province of Bolzano/Bozen created in Easy Language. The Province of Bolzano/Bozen is an Italian authority with a special statute, declaring German, Italian and Ladin as its official languages. This body, in fact, administers a territory located in an Italian geographical area that comprises, for historical reasons, these three languages.

The Easy Language information on the Province of Bolzano website, available in both Italian and German[43], is divided into 53 fact sheets, which are grouped according to topics such as work, support services, leisure, health, administrative aspects of the Region, benefits for people with disabilities, cultural and educational opportunities, mobility and housing assistance. Each thematic area is introduced by a short text, also in Easy Language, which explains what information is contained in the specific section.

The Easy Language pages were created by the Provincial administration in cooperation with 'Okay' – the Easy Language Office of the non-profit organisation *Lebenshilfe* (i.e., "live aid") based in Bolzano[44]. The scientific rules of the Research Centre for Easy Language (University of Hildesheim/Germany)[45] were used for the German Easy Language texts. The texts were proof-read by readers with learning difficulties who work for the "People First" association[46]. This corresponds to the advice of empowerment rulesets: Inclusion Europe and, for the German context, *Netzwerk Leichte Sprache* ("Network Easy Language").

The texts in the Italian version of Easy Language are derived from the translation of the German texts, while also applying the guidelines for the Italian language[47]. The Italian texts, like their German counterparts, have been evaluated by people with cognitive disabilities[48].

3.2. Corpus characteristics

From the Province of Bolzano website, as described in the previous section, 26 German fact sheets and their Italian translations were selected (see tab. 1). The fact sheets are divided into expandable sections introduced by a title, facilitating access.

The German source texts (Corpus Bolzano German) were written directly in German Easy Language. The Italian Easy Language texts (Corpus The fact sheets are divided into expandable sections introduced by a title, facilitating access.

39. Wiesmann 2019.
40. Maaß–Rink–Zehrer 2014.
41. Deilen et al. 2023, Deilen et al. 2024.
42. See Nitzke–Hansen-Schirra 2021 for interlingual translation of standard and expert language texts.
43. See Province of Bolzano Easy Language website in Italian and in German.
44. See OKAY's website.
45. As published in Maaß 2015 and Bredel–Maaß 2016-a, Bredel–Maaß 2016-b.
46. See further information on the Province of Bolzano website.
47. Sciumbata 2022.
48. Melchiori–Siemons 2024; on the reviewing process for Easy language see García Muñoz 2022, Schiffler 2022.

Text-ID	Information sheet title (English translation)	Information sheet title (German)	Information sheet title (Italian)
1	Finding work in South Tyrol	Arbeit finden in Südtirol	Trovare lavoro in Alto Adige
2	Finding work in South Tyrol for people with disabilities	Arbeit finden in Südtirol für Menschen mit Behinderungen	Trovare lavoro in Alto Adige per persone con disabilità
3	Job coaching	Begleitung am Arbeits•platz – Job•coaching	Accompagnamento sul posto di lavoro – Job•coaching
4	Employment services	Dienste zur Arbeits•beschäftigung	Servizi per l'occupazione lavorativa
5	Social cooperatives	Sozial•genossenschaften	Cooperative sociali
6	Social and educational daycare	Sozial•pädagogische Tages•stätten	Centri diurni socio•pedagogici
7	Social services	Die Sozial•dienste	I servizi sociali
8	Women and violence	Gewalt gegen Frauen	Donne e violenza
9	Accessible nature	Barriere•freie Natur	Natura senza barriere
10	Recreation and sport for people with disabilities	Freizeit und Sport für Menschen mit Behinderungen	Tempo libero e sport per persone con disabilità
11	South Tyrol for all	Südtirol für alle	Alto Adige per tutti
12	The medical certificate for sport	Ärztliches Zeugnis für Sport	Il certificato medico per lo sport
13	Coronavirus	Corona	Corona
14	Health districts	Gesundheits•sprengel	Distretti sanitari
15	Doctors and general practitioners	Haus•ärztinnen und Haus•ärzte	Mediche e medici di famiglia
16	Psychological service	Psychologische Dienste	Il servizio psicologico
17	Exemption from co-payment	Ticket•befreiung	Esenzione dal pagamento del ticket
18	Living will	Patienten•verfügung	Il testamento biologico
19	Provincial elections 2023 in South Tyrol	Landtags•wahlen 2023 in Südtirol	Elezioni provinciali 2023 in Alto Adige
20	The administration of the Province of Bolzano	Die Südtiroler Landes•verwaltung	L'Amministrazione della Provincia di Bolzano
21	Social services in South Tyrol	Die Sozial•dienste in Südtirol	I servizi sociali in Alto Adige
22	Income and assets declaration	EEVE - Einheitliche Einkommens•erklärung und	DURP-Dichiarazione unificata di reddito e di patrimonio
23	Employment benefits for people with disabilities	Begünstigungen am Arbeits•platz für Menschen mit Behinderungen	Agevolazioni sul posto di lavoro per persone con disabilità
24	Provincial Law No. 7 of 14 July 2015: Participation and Inclusion of Persons with Disabilities	Landes•gesetz Nummer 7 vom 14. Juli 2015: Teilhabe und Inklusion von Menschen mit Behinderungen	Legge provinciale numero 7 del 14 luglio 2015: partecipazione e inclusione delle persone con disabilità
25	Care allowance	Pflege•geld	Assegno di cura
26	Reimbursement of transport costs and care expenses for people with disabilities	Geld•beiträge für Transport und Begleit•personen von Menschen mit Behinderungen	Contributi per il trasporto e gli accompagnatori delle persone con disabilità

Tab. 1 — *Text IDs and Information sheet titles (English translation, original German and Italian titles)*

The German source texts (Corpus Bolzano German) were written directly in German Easy Language. The Italian Easy Language texts (Corpus Bolzano Italian) are target texts of an interlingual translation process of the German Easy Language texts. As part of the study, Corpus Bolzano German was then translated into Italian using DeepL. The style was set to "automatic". In addition, Corpus Bolzano Italian was translated into German using DeepL. No post-editing was carried out. The German and Italian sub-corpora therefore serve as a gold standard for evaluating the performance of DeepL.

The German and Italian corpus Bolzano are of comparable quality (and therefore both considered "gold standard") because, as stated in the description of the source corpus, the original Italian texts, although derived from a German translation, were aligned with the Italian Easy Language guidelines and tested for user comprehensibility.

The corpus of German texts contain a total of 23.596 words and 134.582 characters, while the corpus of Italian texts consists of a total of 32.011 words and 151.894 characters, distributed among the corpora as shown in the tables 2 and 3.

3.3. Procedure of analysis

In the next step, the results of the two machine translation processes were compared with the gold standard:

- Corpus Bolzano German as gold standard with Corpus DeepL German
- Corpus Bolzano Italian as gold standard with Corpus DeepL Italian.

The procedure of analysis is shown in Fig. 1.

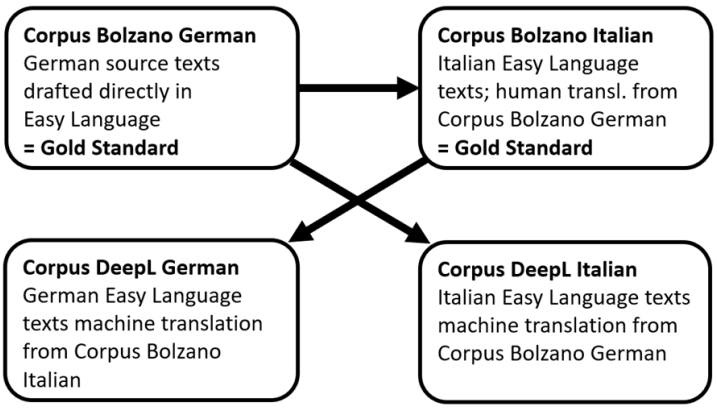

Fig. 1 — *Scheme of the process of comparison of gold standard texts with DeepL translated texts*

The performance of the machine translation can then be determined based on the existence of the Gold Standard texts, which were created exclusively with human resources.

The two sub-corpora were compared with regard to the following properties:

1) Formal readability scores according to the HIX (Corpus Bolzano German and Corpus DeepL German) and according to the Read-it global index (Corpus Bolzano Italian and Corpus DeepL Italian).
2) Correctness with reference to content.
3) Compliance with and deviation from the rules of German and Italian Easy Language.

Regarding the errors identified in the texts translated with DeepL in points 2 and 3, the study aimed to provide qualitative results, highlighting the types of errors and deviations from the EL rules in the target text. The research did not seek to quantify errors or assess their severity as we assumed that if a text contains an error it would be unsuitable for readers.

The results of the analysis are presented in the following section.

4. Results

4.1. Readability scores

The readability score for the German language (Corpus Bolzano German and Corpus DeepL German) was assessed according to the Hohenheim Readability Index (HIX).

	Number of words	Number of characters		Number of words	Number of characters
Corpus Bolzano German	12,416	69,616	Corpus Bolzano Italian	16,558	77,077
Corpus DeepL German	11,180	64,966	Corpus DeepL Italian	15,453	74,817

Tab. 2 — *Number of words and character of the corpora*

Text-ID	Corpus Bolzano German N° of tokens/ N° of sentences/ Average sentence length (in tokens)	Corpus DeepL German N° of tokens/ N° of sentences/ Average sentence length (in tokens)	Corpus Bolzano Italian N° of tokens/ N° of sentences/ Average sentence length (in tokens)	Corpus DeepL Italian N° of tokens/ N° of sentences/ Average sentence length (in tokens)
1	374/54/7.06	336/49/6.86	465/55/8.5	483/55/8.8
2	1,381/191/7.23	1,330/186/7.15	1,830/201/9.1	1.688/197/8.6
3	433/55/7.9	370/52/7.12	502/56/9	457/55/8.3
4	339/44/7.7	288/41/7.02	379/44/8.6	341/44/7.8
5	556/75/7.9	471/67/7.03	650/71/9.2	588/72/8.2
6	338/42/8.05	356/45/7.91	450/44/10.2	398/43/9.3
7	270/47/5.74	261/47/5.55	392/50/7.8	374/50/7.5
8	302/36/8.39	304/38/8	373/55/6.8	327/50/6.5
9	237/40/5.92	283/44/6.43	362/45/8	321/42/7.6
10	853/133/6.41	840/128/6.56	1,199/148/8.1	1,102/143/7.7
11	676/109/6.20	613/107/5.73	874/117/7.5	895/116/7.7
12	976/143/6.83	1,045/139/7.52	1,300/150/8.7	1,230/147/8.4
13	290/42/6.90	302/40/7.55	344/44/7.8	344/46/7.5
14	430/54/7.96	402/53/7.58	547/59/9.3	519/61/8.5
15	311/40/7.78	297/42/7.07	400/43/9.3	378/43/8.8
16	444/70/6.34	446/68/6.56	599/84/7.1	561/83/6.8
17	344/50/6.88	352/50/7.04	464/55/8.4	439/56/7.7
18	634/83/7.64	632/86/7.35	832/94/8.9	735/88/8.4
19	625/80/7.81	609/78/7.81	799/99/8.1	739/90/8.2
20	249/28/8.89	232/30/7.73	302/31/9.7	304/29/10.5
21	270/47/5.74	257/46/5.59	386/49/7.9	371/50/7.4
22	411/55/7.47	399/56/7.12	512/62/8,3	500/59/8,5
23	277/38/7.29	269/35/7.69	377/40/9.4	340/40/8.5
24	615/89/6.91	591/88/6.72	771/96/8	728/92/7.9
25	754/102/7.39	777/112/6.94	1,097/120/9.1	960/11/8.6
26	270/34/7.94	262/34/7.71	352/58/9.3	338/37/9.2

Tab. 3 — *Total number of tokens and sentences and average sentence length for each text of the German and Italian corpora*

The Hohenheim readability Index (HIX) is an index for formally measuring the readability of texts[49]. It contains various relevant readability formulae and other linguistic characteristics for word and sentence length (sentence length, information density, word length, abstracta, etc.). Texts with maximum readability are awarded 20 points. 18 points are the threshold for Easy Language (Rink 2020). Tab. 4 shows the HIX values for the texts from the German corpora in the project.

In the source texts from Corpus Bolzano German, only one out of 26 texts (3,8%) did not achieve the score for Easy Language, while 96,2% performed within the formal Easy Language standard of 18 points or beyond. In the retranslated target texts from the Corpus DeepL German sub-corpus, 10 out of 26 texts (38%) do not meet the formal requirements for Easy Language according to HIX, while only 62% met the formal criteria for Easy Language. Some of the texts clearly miss the 18-point threshold and score below 13 or 14 points, which are standard text readability values that miss the requirements for Easy Language to a considerable extent.

The readability score for the Italian corpora (Corpus Bolzano Italian and Corpus DeepL Italian) was assessed according to the Global Read-IT Index. The Global Read-IT Index is an index designed to measure the readability of a text in Italian. It takes into account a combination of different features, ranging from general text characteristics (sentence and word length) to lexical and syntactic ones. The index score is scaled from 0% for a text considered easy to 100% for a text considered difficult[50].

The readability analysis of the Italian texts was carried out using the online version of Read-it[51], a tool developed by the Italian Natural Language Processing Laboratory of the Institute for Computational Linguistics (ILC) of the National Research Council of Italy[52]. The tool has already been successfully used for the analysis of legal texts[53].

Tab. 5 shows the Global Read-IT index values for the texts from the Corpus Bolzano Italian and Corpus DeepL Italian.

Text-ID	Corpus Bolzano German	Corpus DeepL German
1	19.25	19.34
2	19.12	18.89
3	20.00	18.10
4	20.00	19.24
5	20.00	13.92
6	18.84	16.96
7	18.12	12.43
8	18.84	19.08
9	20.00	19.90
10	19.47	17.74
11	19.84	19.96
12	19.60	19.47
13	19.33	19.02
14	18.11	17.11
15	19.16	19.67
16	19.94	19.26
17	19.35	18.16
18	19.13	18.27
19	18.87	18.92
20	17.17	17.14
21	18.12	12.44
22	19.13	19.70
23	18.79	15.84
24	19.15	16.87
25	19.05	19.81
26	18.70	16.21

Tab. 4 — *HIX scores for the two German corpora*

There is no formally established benchmark for Easy Language for Italian. For the purposes of this study, comparability with the HIX is assumed as a working hypothesis. According to the HIX, 18 out of 20 points must be achieved in order to be considered Easy Language. This corresponds to a maximum deviation of 10% from the maximally

49. Kercher 2013, Hansen-Schirra–Gutermuth 2018; Bredel–Maaß 2016-a.

50. Dell'Orletta–Montemagni–Venturi 2011.

51. See the Read-it demo available for the Italian language.

52. *Ibidem*.

53. Brunato–Venturi 2014.

achievable score. For the Global Read-IT, this deviation corresponds to a maximum value of 10%.

Even though this remains a working hypothesis, this score is plausible since the complexity of an Easy Language text – designed for individuals with cognitive disabilities – is significantly lower than that of an average comprehensibility text (Global Read-it Index score: 50%).

In the Corpus Bolzano Italian, 9 of the 26 texts scored more than 10% and were thus outside the assumed formal framework of Easy Language. This corresponds to 34.6%, i.e., only 65.4% of the Italian texts met these criteria.

In the corpus DeepL Italian, 12 out of 26 texts scored outside the presumed Easy Language frame. This corresponds to 46.1%, which means that only 53.8% of the texts fulfil the criterion. Some of the texts in Corpus DeepL Italian break the 10% threshold very clearly and score considerably higher than the less easy texts in Corpus Bolzano Italian. The least easy text in Corpus Bolzano Italian reaches 35%, in Corpus DeepL Italian it is 84,9%. It can be seen here that the texts have been normalised towards the standard: the automated translation with DeepL has increased their complexity, making them more similar to typical administrative texts.

Text-ID	Corpus Bolzano Italian	Corpus DeepL Italian
1	1.8%	6.8%
2	1.3%	8.3%
3	0.7%	3.2%
4	1.2%	3.0%
5	6.8%	9.4%
6	0.1%	0.5%
7	6.1%	9.4%
8	16.5%	65.2%
9	15.2%	41.3%
10	11.4%	21.2%
11	19.0 %	27.3%
12	2.8%	6.4%
13	13.9%	31.9%
14	10.9%	42.2%
15	0.7%	0.7%
16	35.8%	84.9%
17	3.2%	27.5%
18	3.7%	39.2%
19	22.8%	50.0%
20	3.8%	1.6%
21	5.7%	19.4%
22	5.1%	6.0%
23	0.1%	1.3%
24	10.06%	18.6%
25	1.4%	5.9%
26	1.0%	7.7%

Tab. 5 — *Read-IT scores for the two Italian corpora*

4.2. Correctness

The verification carried out on the Easy Language texts translated with DeepL revealed a number of critical points regarding their correctness (which is in line with the results in Deilen et al. 2023 and Deilen 2024 for intralingual translation). These findings were convergent in the two translation directions (German-Italian and Italian-German). The salient categories are presented below and illustrated with examples.

4.2.1. Semantic shifts through non congruent synonymy

Both DeepL corpora contain errors that result from the fact that certain terms in the respective source language have a different scope and an equivalent that is inappropriate for the context that appears in the target language. This is the case in the following example where Italian "laboratorio" has both the meaning "laboratory" and "sheltered workshop". So for the Italian source text, "laboratorio" is correct. In the German context, "Werkstatt", that is "sheltered workshop" is needed, but Corpus DeepL German-4 gives "Labor" ("laboratory") instead (see 1).

(1)

Corpus Bolzano German-4	Corpus DeepL German-4
Was machen die Menschen in der Werkstatt?	Was machen die Menschen im Labor?
What do people do in the sheltered workshop?	*What do people do in the laboratory?*

This type of error is also found in the Italian translations: for example, in Corpus Bolzano Italian-2 the word "indennità" ("allowance") is replaced in DeepL Italian-2 by "paghetta" ("child's pocket money") (see 2).

(2)

Corpus Bolzano Italian-2	Corpus DeepL Italian-2
Nel progetto di integrazione l'azienda paga alla persona con disabilità un'indennità. *In the work integration project the company pays persons with disabilities an allowance.*	Nel progetto di integrazione l'azienda dà alle persone con disabilità una paghetta. *In the work integration project the company gives persons with disabilities child's pocket money.*

4.2.2. Translation of proper names and terms

Another critical aspect of the Deepl-translated versions, in both languages, concerns technical or specific terminology that cannot be expressed as such by synonyms, as it would no longer be recognisable in the context to which it belongs. Particularly, this concerns names relating to legal institutes and administrative organisations typical of a given country (such as the names of public bodies, offices and services) and names referring to specific professional figures. The particular difficulty here is that the proper names of the municipality of Bolzano are generalised in the direction of the standard for Germany and the actual terms disappear from the Italian in the retranslation. For example, the German "Meldeamt" is translated literally as "registration office", not considering that in Italy the office for the procedure mentioned in the text is called "ufficio anagrafe".

The text Corpus Bolzano German-25 contains the word "Sozial·sprengel", which is separated with a mediopoint according to the Easy Language rules for long words[54]; DeepL replaces this term with two other terms and does not even preserve term consistency as an additional problem (see 3).

(3)

Corpus Bolzano German-25	Corpus DeepL German-25
Oder bei Ihrem Sozial•sprengel. Die Liste mit den Sozial•sprengeln in Südtirol finden Sie hier. *Or at your local social welfare centre.* *You can find the list of welfare centres in South Tyrol here.*	Oder bei den Ämtern Ihres Sozialhilfebezirks. Hier finden Sie die Liste der Sozialbezirke in Südtirol. *Or at the offices of your social welfare district.* *Here you can find the list of social districts in South Tyrol.*

The machine-translated text is not sufficiently action-oriented[55], as it remains unclear to text users which office is to be addressed. In order to carry out the action successfully, it is necessary to know the correct terminology, which is used, for example, in the forms to be filled out. Reproduction with different terminology considerably reduces the action-orientation of the texts.

A corresponding example for the Italian language is the term "Distretti sanitari" ("Health districts", Corpus Bolzano Italian-14) that appears as "Centri sanitari" ("Health center") in Corpus Bolzano DeepL-14 (see 4).

54. See Bredel–Maaß 2016-a, Bredel–Maaß 2017.

55. Maaß 2020; Maaß–Rink 2021.

(4)

Corpus Bolzano Italian-14	Corpus DeepL Italian-14
Dove sono i distretti sanitari? *Where are the health districts?*	Dove sono i centri sanitari? *Where are the health centers?*

4.2.3. Use of modal verbs

In the texts produced by DeepL, specific critical points were found in the translation of modal verbs. These are sometimes modified with respect to the source text, resulting in a considerable semantic shift in the text, both in the German and the Italian corpora (see 5).

(5)

Corpus Bolzano German-8	Corpus DeepL German-8
Oder diese Frauen dürfen nicht aus dem Haus gehen. *Or those women must not leave the house.*	Oder diese Frauen können nicht aus dem Haus gehen. *Or those women cannot leave the house.*

In Corpus Bolzano Italian-5 the expression "devono guadagnare soldi" ("must earn money") appears as " vogliono guadagnare soldi" (Corpus DeepL-5), that is "want to earn money", thereby losing the meaning that it is a right (and not just a desire) to receive remuneration for the work done (see 6).

(6)

Corpus Bolzano Italian-5	Corpus DeepL Italian-5
Anche le cooperative sociali devono guadagnare soldi. *Even social cooperatives must earn money.*	Anche le cooperative sociali vogliono guadagnare soldi. *Even social cooperatives want to earn money.*

4.2.4. Grammatical errors

In some cases, the machine translated versions reported grammatical problems. These are errors that are limited in number but recur in the same syntactic structures. This is the case in the following German example, in which the auxiliary+infinitive structure "wählen können" ("can vote") occurs twice:

(7) Wählen können auch Menschen, die die einen Vormund oder Betreuer haben, können auch wählen gehen. (Corpus Bolzano German-19)
**Vote can also people that have a legal guardian can vote*.

The same is true for the next Italian example, where the "bullet point" structure, that is typical for Easy Language texts, has an introductory sentence that does not grammatically match the following list of elements. It seems as though the translation did not recognise the two parts to be syntactically connected:

(8) "Le persone possono stare nel centro diurno: (*People can stay in the day centre*)
- stare insieme ad altre persone (*be with other people*)
- imparare cose nuove (*learn new things*)
- e fare cose interessanti (*and do interesting things*)" (Corpus DeepL Italian-6).

4.2.5. Non-translated sequences

Another category of errors found in the text concerns sequences of words which, in both directions of translation, have remained unchanged in relation to the source text, albeit to a very limited extent, thus appearing in Italian in the German text and in German in the Italian text. This applies, for example, to the names of the Bolzano administrative units, which in the machine translation remain in German in the Italian text and in Italian in the German text, but not consistently. The names that have been correctly translated are shown in bold, the untranslated cases are underlined (see 9).

(9)

Source text: Corpus Bolzano German-7	Target text: Corpus DeepL Italian-7
Die 8 Sozial•dienste sind: – Betrieb für Sozial•dienste in **Bozen**. – Sozial•dienst Burggrafenamt. – Sozial•dienst Eisacktal. – Sozial•dienst **Pustertal**. – Sozial•dienst Salten-Schlern. – Sozial•dienst Überetsch-Unterland. – Sozial•dienst **Vinschgau**. – Und Sozial•dienst Wipptal.	Gli 8 servizi sociali sono: – Operazione per i servizi sociali a **Bolzano**. – Servizio sociale del Burggrafenamt. – Servizio sociale Eisacktal. – Servizio sociale della **Val Pusteria**. – Servizio sociale di Salten-Schlern. – Servizio sociale Überetsch-Unterland. – Servizio sociale della **Val Venosta**. – E il servizio sociale Wipptal.

The problem is also reproduced in the other translation direction. Here it also becomes clear that there is no system underlying it, because different toponyms are translated or left untranslated in the German-Italian translation than in the other direction (see 10).

(10)

Source text: Corpus Bolzano Italian-7	Target text: Corpus DeepL German-7
In Alto Adige ci sono 8 servizi sociali: – Azienda servizi sociali di **Bolzano**. – Servizi sociali del **Burgraviato**. – Servizi sociali della **Val d'Isarco**. – Servizi sociali della **Val Pusteria**. – Servizi sociali Salto-Sciliar. – Servizi sociali Oltradige-Bassa Atesina. – Servizi sociali della **Val Venosta**. – E servizi sociali dell'Alta Val d'Isarco.	In Südtirol gibt es 8 Sozialdienste: – Die Sozial-Dienste von **Bozen**. – Sozialdienst **Burggrafenamt**. – Sozialdienst des **Eisacktals**. – Sozialdienst **Pustertal**. – Sozialdienst Salto-Sciliar. – Sozialdienst Oltradige-Bassa Atesina. – Sozialdienste **Vinschgau**. – Und Sozialdienste Alta Val d'Isarco.

4.2.6. Abbreviations

Abbreviations remain untranslated throughout the target texts. In a bilingual region such as Bolzano, however, each language has its own abbreviations for the same institutions and processes in the administrative context, which are usually based on the unabbreviated compound. These abbreviations therefore remain as leftovers in the automatically translated target text. The risk exists that they will not be recognised or that they cannot be related to the unabbreviated compound if this also appears in the text. In the following example, the abbreviation is resolved differently on two occasions in the translation – once even in English (see below for English fragments in the translation), both times without reference to the individual letters of the abbreviation (see 11).

(11)

Corpus Bolzano Italian-22	Corpus DeepL German-22
DURP – Dichiarazione unificata di reddito e patrimonio. DURP è la sigla per: **D**ichiarazione **u**nificata di **r**eddito e **p**atrimonio.	**DURP - Einheitliche Erklärung über Einkommen und Vermögen.** DURP steht für: Unified Declaration of Income and Assets (Einheitliche Erklärung über Einkommen und Vermögen).

The problem also applies to the reverse translation direction. This case is specific for the fact that in one case the abbreviation is not even correctly transferred to the target text: in the heading, EEVE becomes EVE, while the correct German abbreviation appears in the Italian body text below (see 12).

(12)

Corpus Bolzano German-22	Corpus DeepL Italian-22
EEVE - Einheitliche Einkommens•erklärung und Vermögens•erklärung.	**EVE - Dichiarazione Unica di Reddito• e Patrimonio•.**
EEVE ist die Abkürzung für: **E**inheitliche **E**inkommens•erklärung und **V**ermögens•**e**rklärung.	EEVE è l'abbreviazione di: Dichiarazione Uniforme dei Redditi e Dichiarazione dei Patrimoni.

It is obvious that these cases considerably restrict the action orientation because the abbreviation cannot be resolved in the respective context of the other language.

4.2.7. English fragments in the translation

Both the Italian and the German DeepL corpora display some fragments of English with no relation to the source text. We have seen an example for the translation direction Italian > German in (11) above. An example for the translation direction German > Italian is the following, where the English term "exemption" appears in the Italian title – instead of "esenzione" (see 13).

(13)

Corpus Bolzano German-17	Corpus DeepL Italian-17
Ticket•befreiung.	**Ticket exemption.**
Ein Ticket ist ein Geld•beitrag. Diesen Geld•beitrag bezahlen Menschen zum Beispiel für Untersuchungen im Kranken•haus. Untersuchungen können nämlich viel Geld kosten. Die Menschen müssen nicht die ganze Untersuchung bezahlen. Die Menschen bezahlen nur einen Teil. Dieser Teil heißt: Ticket.	Un biglietto è un contributo monetario. Le persone pagano questo contributo in denaro• per per le visite in ospedale, ad esempio. Gli esami possono costare molto. Le persone non devono pagare per l'intero esame. Si paga solo una parte. Questa parte si chiama ticket.

In the target text, "ticket" is sometimes rendered as "ticket" and sometimes as "biglietto"; this inconsistency makes it considerably more difficult to build up a mental representation of the subject. The requirement of term consistency is a rule of Easy Language, which we will discuss below. However, it is obvious here that problematic results arise at text level even beyond the requirements of Easy Language. The presence of the English language could perhaps be due to the fact that DeepL uses English as a pivot language for some translations[56].

4.3. Deviation from the German/Italian Easy Language guidelines

Easy Language is highly regulated and deviates from the standard varieties of natural languages in the extent of these regulations[57]. However, DeepL does not carry out its translations on the basis of the Easy Language rule system, but on the basis of dominant standard language and specialised language text corpora[58]. The input texts of the Bolzano Corpus are in Easy Language and we have shown above that the machine translated target texts are still relatively easy, even if on average they no longer meet the Easy Language benchmark. This section offers a qualitative analysis of the aspects in which the target texts deviate from the standard requirements of Easy Language.

4.3.1. Normalisation towards the standard

As was to be expected, we can observe an overall normalisation of the target texts towards the

56. Gerhalter 2024.

57. For a short cross-language summary of the basic rules, see Maaß 2024-a, p. 238 f.

58. For a quantitative study of the error types in the respective corpora see Maaß–Fioravanti 2025.

standard for administrative texts. The sentences are longer and the vocabulary is less commonplace and does not belong to the fundamental vocabulary of German[59] or Italian[60]. This is particularly evident where the target texts show more complex synonyms for the same subject than the Gold Standard texts. The corpus contains numerous examples of this phenomenon in both translation directions, including the following (see 14).

(14)

Corpus Bolzano German-18	Corpus DeepL German-18
Eine Patienten•verfügung kann verschieden gemacht sein.	Eine Patientenverfügung kann auf viele verschiedene Arten verfasst werden.

The example shows another striking feature of the corpus: a special rule of German Leichte Sprache is the splitting of long words with hyphens or mediopoints[61]. The Bolzano corpus follows the rules of the Research Centre for Easy Language of the University of Hildesheim and therefore works with mediopoints. The Italian human translation (Bolzano Italian corpus) partially adopts these and is therefore the only corpus of Italian Easy Language known to us with this feature. But wherever there are no mediopoints in the Italian source text, they are also missing in the German Easy Language text – even in long compounds such as in this example, where they are obligatory for German Easy Language.

Example 15 gives a list of Italian words that have been substituted by terms belonging to a higher linguistic register or by hyponyms that don't belong to the Italian basic vocabulary (see 15).

(15)

Corpus Bolzano Italian	Corpus DeepL Italian
medicina (*medicine*)	farmaco (*medication*)
persona (*person*)	dipendente (*employee*)
andare (*to go*)	recarsi (*"to go" higher linguistic register*)
fare un lavoro (*to do a job*)	svolgere un lavoro (*to perform a job*)
cose (*things*)	beni (*goods*)

In the Italian machine-translated version, as regards nouns, for example, in the information sheet on the "Administration of the Province of Bolzano" the word "persona" ("person") is replaced by the more specific and elevated term "dipendente" ("employee"), while in the information sheet on the "Medical certificate for sports", the basic Italian word "medicina" ("medicine") appears in the machine-translated version as "farmaco" (a highly used word but not belonging to the fundamental vocabulary). Another example of substitution with more complex nouns can also be found in the information sheet on the "Unified declaration of income and assets", where "cose" ("things") become "beni" ("goods").

In the case of verbs, there is also a tendency to use more complex terms in the automatically translated texts. For example, in the information sheet on finding a job, "fare un lavoro" (to do a job) becomes "svolgere un lavoro" ("to perform a job"), while in the one on psychological services "fare un test" ("to do a test") becomes "eseguire un test" ("to

59. Its qualities are described in Bredel–Maaß 2016-a, p. 347 ff.

60. See De Mauro 2003; Chiari–De Mauro 2014.

61. The "mediopoint" was proposed for German Easy Language in Maaß 2015 and Bredel–Maaß 2016-a, b "to segment compounds where the use of the hyphen would be incorrect. The mediopoint is not part of the German orthographical system and thus more neutral, as it does not generate misspellings in the strict sense. Just like the hyphen, it indicates the borders between the single lexical items in the compound noun" (Maaß 2020).

carry out a test"). The verb "andare" ("to go") as in "andare al distretto sanitario" is then replaced by synonyms belonging to a higher linguistic register, such as "recarsi" or "rivolgersi" ("to address") as in "rivolgersi alla commissione medica".

4.3.2. Verbal tenses, modes and diathesis

Verbal tenses and modes are strongly restricted in Easy Language. Bredel and Maaß[62] show that the practical rules for German are limited to the present and perfect tenses and the indicative, while the subjunctive should not be used. In Italian, the subjunctive is obligatory in some grammatical constructions, so it cannot generally be avoided; the limitation to only one past tense is also not grammatically possible. Nevertheless, even in Italian, Easy Language limits itself to the minimum possible number of tenses and modes and avoids morphological complexity wherever possible[63]. This limitation is not found in the automatic translations: We find many examples for verbal tenses and modes that are more complex than the ones suggested in the Easy Language guidelines. This includes conditional and gerund as well as future tense and passive constructions (see 16).

(16)

Corpus Bolzano German-19	Corpus DeepL German-19
Die Broschüre ist vom Südtiroler Landtag. *The brochure is from the South Tyrolean Parliament.*	Dieser Text wurde vom Landesrat verfasst. *This text was compiled by the Provincial Council.*

In this case, the present active "is" was substituted by a past tense passive. The following example has future tense instead of present (see 17).

(17)

Corpus Bolzano Italian-19	Corpus DeepL Italian-19
Le elezioni provinciali in Alto Adige sono il 22 ottobre 2023. *The provincial election in South Tyrol is on 22 October 2023.*	Il 22 ottobre 2023 si terranno le elezioni provinciali in Alto Adige. *The provincial election in South Tyrol will be held on 22 October 2023.*

4.3.3. Impersonal constructions and double negatives

Impersonal sentences are more complex than personal sentences because they conceal the subject of the sentence and do not address the reader[64]. Easy Language texts should be written in an action-orientated way[65]: users should understand who the actors and contact persons are in the administrative context. For this reason, impersonal constructions as well as passive constructions are not allowed in the Easy Language rulesets[66].

In the following German example, the formal form of addressing is used throughout the human translation. This ensures action-orientation and politeness. In the DeepL version, the title uses the impersonal form, which is not part of the repertoire of Easy Language. The next sentence switches to the informal form of address, which signals closeness if used among family and friends, but communicates asymmetry in an administrative context (see 18).

62. Bredel–Maaß 2016-a.
63. Sciumbata 2022.
64. *Ibidem*.
65. Maaß 2020, p. 47 ff.
66. Bredel–Maaß 2016-a, p. 506 ff.; Maaß 2024-a.

(18)

Corpus Bolzano German-22	Corpus DeepL Italian-22
Was brauchen Sie für die EEVE?	Was braucht man, um DURP zu machen?
Sie brauchen viele Dokumente.	Um DURP zu machen, brauchst du viele Dokumente.
What do you [formal pronoun] need for the EEVE?	*What does one need in order to do DURP?*
You [formal pronoun] need many documents.	*In order to do DURP, you [informal pronoun] need many documents.*

Formal addressing is also used in the Italian Gold Standard Corpus. This is unusual, as in the Italian context informal addressing is also used in administrative interaction. Formal addressing is therefore less close to everyday life. Here, the avoidance of asymmetry and the observance of formal politeness were obviously prioritised over comprehensibility. An impersonal form appears in the machine-translated version: (see 19).

(19)

Corpus Bolzano Italian-14	Corpus DeepL Italian-14
Lei ha l'esenzione del ticket?	Si ha diritto all'esenzione del ticket?
Do you [formal pronoun] have a fee exemption?	*Is one entitled to a fee exemption?*

Practical guidelines also advise against negative statements and negation in general. Research has shown that this is not expedient[67] if a statement is conceptually negative, it is action-orientating if this negativity is also evident on the linguistic surface. Another case is double negatives: here, an actually positive statement is presented on the linguistic surface with a (double) negative statement. Such uses of negation are not advisable for Easy Language. However, such double negatives can be found in machine-translated texts in the corpus, as in the following example (see 20).

(20)

Corpus Bolzano Italian-19	Corpus DeepL Italian-19
Per votare lei ha bisogno di una tessera elettorale.	Non è possibile votare senza la tessera elettorale.
To vote you need a voter registration card.	*You cannot vote without a voter registration card.*

4.3.4. Same concept – same designation

The Easy Language guidelines recommend using the same designation for the same concepts throughout the document, in order to support text cohesion and the correct interpretation of concepts[68]. This rule is broken in almost every single text in both automatically translated sub-corpora. It is clear that DeepL operates on a sentence basis and does not establish consistency even at section level, let alone at text level. Examples of this in the preceding text include (12), (13) and (14). In the following, we give one more example for each language (see 21 and 22).

67. Bredel–Maaß 2016-a, p. 460 ff.; Maaß 2020, p. 74 ff.

68. Maaß 2020, p. 103 ff.; Sciumbata 2022.

(21)

Corpus Bolzano German-12	Corpus DeepL German-12
Nicht•leistungs•sport *non-competitive sport*	Sport ohne Wettkampfcharakter, Freizeitsport, wettbewerbsfreier Sport, Nicht-Wettkampfsport *non-competitive sport, recreational sport, uncompetitive sport, non-competition sport*

(22)

Corpus Bolzano Italian-15	Corpus DeepL Italian-15
medico di famiglia *family doctor*	medico di famiglia, medico di base *family doctor, general practitioner*

4.3.5. Non-explanation or wrong explanation of difficult terms

Easy Language texts avoid using technical or unfamiliar words[69]. However, in administrative texts, it may be necessary to include such words[70]. In this case, they should be clearly explained the first time they appear in the text[71], as has been done in the German and Italian Bolzano Corpora. In Corpora DeepL, this rule is violated when the difficulty level of a word doesn't correspond between the two languages, causing two types of problems: (1) if the source text does not contain an explanation, there will be none in the automated translation (even though the word used in the translation would need one); (2) if the word in the target text does not require an explanation, there will be one anyway, and it will either be incorrect or make the text heavier (see 23).

(23)

Corpus Bolzano German-7	Corpus DeepL German-7
Die Sozial•sprengel sind in Häusern. In diesen Häusern arbeiten viele Menschen. Diese Menschen sind Fach•personen vom Sozial•sprengel. Die Fach•personen unterstützen die Menschen bei Problemen. *The social centres are located in houses.* *Many people work in these centres.* *These people are specialists from the Sozialsprengel.* *The specialists support people with problems.*	Sozialbezirke befinden sich in Gebäuden. Gebäude ist ein anderes Wort für: Zuhause. *Social districts are located in buildings.* *Building is another word for: Home.*

An Italian example for an incorrect or useless explanation is (24).

69. Maaß 2024-a.

70. Rink 2020.

71. Maaß 2020; Rink 2020; Sciumbata 2022.

(24)

Corpus Bolzano Italian-23	Corpus DeepL Italian-23
L'azienda ha tante sedi. Sedi significa: L'azienda lavora in tanti posti diversi. *The company has many locations, Locations means: the company works in many different places.*	L'azienda ha molte sedi. Sedi significa: L'azienda ha molte sedi. *The company has many locations.* *Locations means: The company has many locations.*

5. Summary and Discussion

For the language pair German-Italian, the study analysed how DeepL performs in interlingual translation with texts in Easy Language as the source text. Corpus Bolzano German is a sub-corpus comprising 26 texts that was created directly in Easy Language according to the scientific rules of the Research Centre for Easy Language. Corpus Bolzano Italian is the human translation of these texts into Italian Easy Language. These two sub-corpora served as the Gold Standard for comparison with the machine-translated sub-corpora Corpus DeepL German and Corpus DeepL Italian created for the purpose of the study. The corpora were analysed according to the following criteria:

1) Readability
2) Correctness
3) Compliance with the Easy Language rules

(1) The results show that DeepL normalises the texts towards the standard at all linguistic levels. However, this also applies to the Italian human translation.

While 96.2% of the texts in Corpus Bolzano German reach the Easy Language threshold, this only applies to 73.1% of the human translations into Italian in Corpus Bolzano Italian. The levelling towards the standard is even stronger for the machine-generated texts: only 62% of the machine-translated texts from Italian in the Corpus DeepL German achieve the minimum readability for Easy Language. And only 53.8% of the texts translated from German in the corpus DeepL Italian achieve this minimum value. This figure is subject to an assumed readability of HIX for German and Global Read-it for Italian, whereby 90% of the maximum readabiltiy was assumed as the threshold for Easy Language in each case. Further studies are needed here. Overall, it can be seen that the interlingual machine translation of legal-administrative texts with DeepL tends more towards the standard legal texts than the human translation in the Gold Standard Corpus. The texts are therefore not easy enough.

By normalising the data obtained with the two readability indices on a scale between 0 and 1, we can more easily compare the scores obtained by the two DeepL corpora. In the German DeepL corpus readability decreased from a minimum of 0.002 (0.2%) to a maximum of 0.304 (30.4%). In 7 cases (out of 26) readability increased slightly. Only 6 out of 26 increased their complexity by more than 10%. In the Italian DeepL corpus, readability decreased from a minimum of 0.09 (0.9%) to a maximum of 0.491 (49.1%). In 1 case readability increased slightly. Only 9 out of 26 texts increased their complexity by more than 10% (2 between 10% and 20%, 3 between 20% and 30%; 2 between 30% and 40%; 2 between 40% and 50%). The readability scores obtained from the Bolzano and DeepL corpora for the two languages are compared in the following graphs (fig. 2 and fig. 3). The horizontal line at 0,9 point corresponds to the threshold for Easy Language.

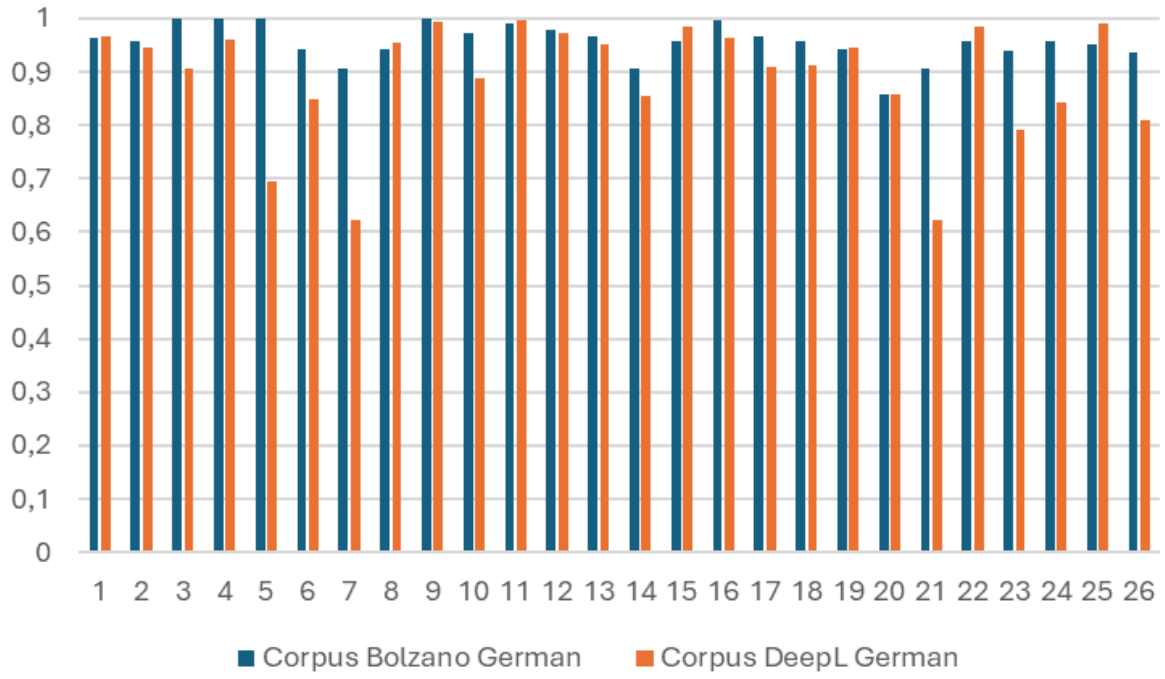

Fig. 2 — *Graph of normalised readability obtained by the Bolzano German and DeepL German corpora*

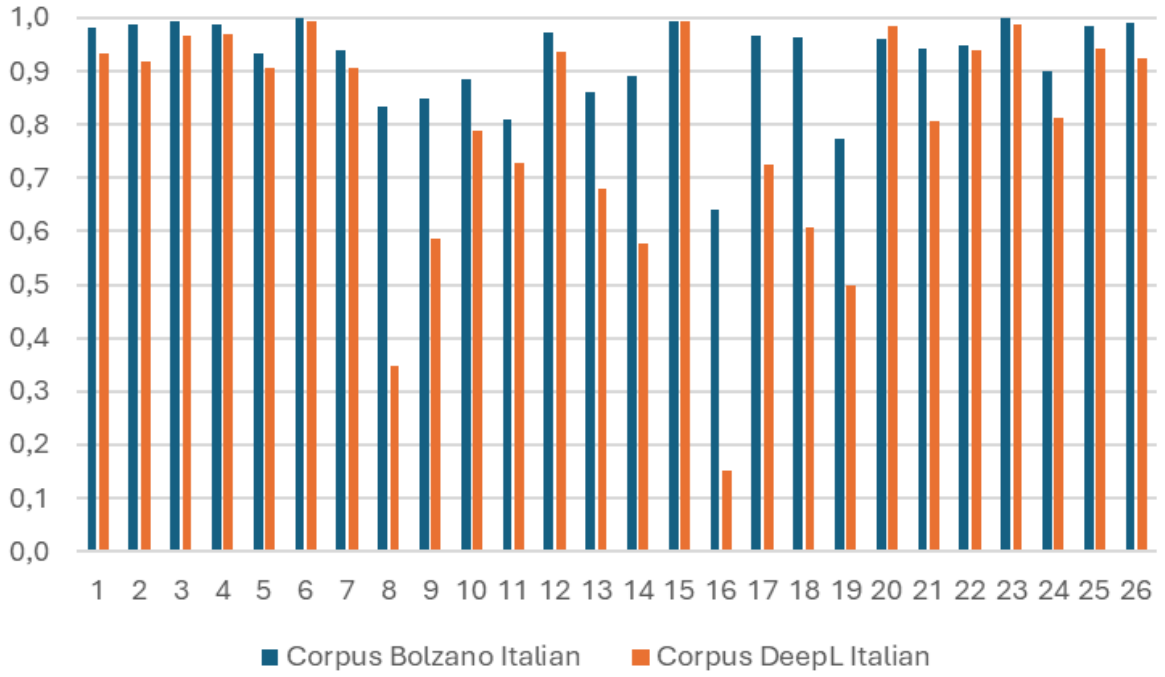

Fig. 3 — *Graph of normalised readability scores obtained by the Bolzano Italian and DeepL Italian corpora*

(2) With regard to the types of error, problems can be seen at all linguistic levels that run through the machine-translated sub-corpora: semantic shifts of terms in all word types, especially in the area of terminology, toponymy, names of institutions and official titles, modal verbs, abbreviations, etc. Grammatical errors were also found in sporadic but recurrent cases in the same syntactic structures. Finally, there were also untranslated fragments that remained in the respective source language, as well as fragments in English. This problem seems to occur particularly with low resource and medium resource languages in machine translation and it would be interesting to

see how the German-Italian language pair is positioned in this context. However, this would require a broader interlingual perspective and larger corpora with more text types. The problems with content correctness are pronounced and show that machine-translated texts pose a security risk for the primary target groups, as the information they contain is not reliable and secure.

(3) With regard to deviations from the Easy Language rules in the Corpora DeepL, these were only identified when the same rules were applied in the corresponding texts of the Bolzano corpora. Deviations from these rules included using more complex terms, verb tenses, modes, double negatives and syntactic structures that are not covered by the Easy Language guidelines since they increase the complexity of the text on word and syntactic levels. With regard to the text level, we noticed pronounced term inconsistencies and an overall deviation from the principle "same concept – same designation" for all word types. The deviations observed show an overall tendency of machine translation to approach the characteristics of typical standard administrative texts[72]. Another striking feature was the non-compliance of term explanations to Easy Language requirements.

It is the nature of machine translation to adhere to the source text and simply adopt the word explanations it contains. As these are often language-specific, the explanations are commonly inappropriate or incorrect for the target text. This is where intralingual text simplification tools and intralingual translation into Plain Language and Easy Language perform significantly better[73]. This is a limiting factor for interlingual translation into Easy Language: explanations of terms have to be processed in post-editing. This involves selecting terms that are important for the target text, redrafting definitions and possibly removing existing definitions from the target text. Explanations of terms therefore represent an effort that should not be underestimated in the context of post-editing tasks. This is likely to have a limiting effect on the efficiency of interlingual Easy Language translation with DeepL.

To summarise, it can be said that DeepL has achieved good, but not outstanding results in interlingual translation into Easy Language administrative texts[74]. The texts harbour the risk of producing non-understanding and misunderstanding among the users from the primary target groups. This happens in two ways: (1) Through incorrect solutions (analysis category 2: correctness); (2) By not being comprehensible enough (analysis category 1: readability/comprehensibility) or by not complying with the Easy Language Rules and thus overstraining users (analysis category 3: compliance with the Easy Language Rules). Misunderstanding is the bigger problem here because users may assume that they have understood, yet base their actions on false assumptions. In the case of open non-comprehension, the text can represent a motivational or emotional barrier because it remains unclear in the specific situation whether the users will invest the energy to obtain further resources. However, non-understanding does not contain the false certainty inherent in misunderstanding.

The automatic translation of texts in Easy Language cannot therefore be proposed directly to the recipient of the information (e.g., by inserting the functionality into an institutional website), as human post-editing is always required to make it accurate and suitable for the target audience. However, the study results suggest that DeepL can surely provide support and be an important tool to help increase the number of Easy Language texts currently available to those needing simplified information. Through interlingual machine translation and post-editing, texts from European countries that already have long experience and a large production of administrative or legal texts in Easy Language[75]. Existing texts could therefore be disseminated to other countries in order to increase the number of texts available to the communities.

72. As described in Maaß–Rink 2021 for German and Fioritto 2009 for Italian.

73. Deilen–Lapshinova-Koltunski– Hernández Garrido 2024.

74. These results therefore differ from those obtained in studies on DeepL translation of standard language, which had achieved excellent performance (see, for example, the studies by Tavosanis 2019 on the translation of journalistic language between Italian and English and by Rescigno–Monti 2023 for the language pair German and Italian, which used the MT-GenEvsal data set based on data from Wikipedia).

75. For the Easy Language text practice in 21 European countries see Lindholm–Vanhatalo 2021.

References

S. Ahrens (2024), *Patientinnenaufklärung beim Frauenarzt. Welche Eigenschaften müssen Einfache-Sprache-Texte haben, um für Frauen mit Deutsch als Zweitsprache verständlich und anwendbar zu sein?*, Manuscript of the PhD thesis. Ph.D. thesis, Univ. of Hildesheim, 2024

S. Ahrens, C. Maaß (2024), *Der Einfluss von Vorwissen und sprachlichen Texteigenschaften auf die Anwendung des Fragebogens in einer gynäkologischen Patientenaufklärung: eine leitfadengestützte Interviewstudie*. In "Prävention und Gesundheitsförderung", 2024

S. Ahrens, C. Fioravanti (2022), *Cultural implications in Easy Language texts for migrants: Theoretical considerations and insights from practice in Germany and in Italy*, in "Trans-kom", vol. 15, 2022, n. 2

U. Bredel, C. Maaß (2017), *Wortverstehen durch Wortgliederung – Bindestrich und Mediopunkt in Leichter Sprache*, in B. Bock, U. Fix, D. Lange (eds.), "Leichte Sprache im Spiegel theoretischer und angewandter Forschung", Frank & Timme, 2017

U. Bredel, C. Maaß (2016-a), *Leichte Sprache. Theoretische Grundlagen, Orientierung für die Praxis*, Duden, 2016

U. Bredel, C. Maaß (2016-b), *Ratgeber Leichte Sprache*, Duden, 2016

D. Brunato, G. Venturi (2014), *Le tecnologie linguistico-computazionali nella misura della leggibilità di testi giuridici*, in "Informatica e diritto", 2014, n. 1

I. Chiari, T. De Mauro (2014), *The New Basic Vocabulary of Italian as a Linguistic Resource*, in R. Basili, A. Lenci, B. Magnini (eds.), "Proceedings of the First Italian Conference on Computational Linguistics CLiC-it 2014", Pisa University Press, 2014

M. Cortelazzo (2019), *Il linguaggio amministrativo. Principi e pratiche di modernizzazione*, Carocci editore, 2019

S. Deilen, S. Hernández Garrido, E. Lapshinova-Koltunski, C. Maaß (2023), *Using ChatGPT as a CAT tool in Easy Language translation*, in S. Štajner, H. Saggio, M. Shardlow, F. Alva-Manchego (eds.), "Proceedings of the Second Workshop on Text Simplification, Accessibility and Readability", INCOMA Ltd., Shoumen, 2023

S. Deilen, E. Lapshinova-Koltunski, S. Hernández Garrido et al. (2024), *Towards AI-supported Health Communication in Plain Language: Evaluating Intralingual Machine Translation of Medical Texts*, in D. Demner-Fushman, S. Ananiadou, P. Thompson, B. Ondov (eds.), "Proceedings of the First Workshop on Patient-Oriented Language Processing (CL4Health) @ LREC-COLING 2024", ELRA and ICCL 2024

F. Dell'Orletta, S. Montemagni, G. Venturi (2011), *READ-IT: Assessing Readability of Italian Texts with a View to Text Simplification*, in N. Alm (ed.), "Proceedings of the Second Workshop on Speech and Language Processing for Assistive Technologies", Association for Computational Linguistics, 2011

T. De Mauro, (2003), *Guida all'uso delle parole. Parlare e scrivere semplice e preciso per capire e farsi capire*, Editori Riuniti, 2003

A. Fioritto (2009), *Manuale di stile dei documenti amministrativi*, il Mulino, 2009

T.N. Fitria (2023), *Performance of Google Translate, Microsoft Translator, and DeepL Translator: Error Analysis of Translation Result*, in "Al-Lisan: Jurnal Bahasa (e-Journal)", vol. 8, 2023, n. 2

Ó. García Muñoz (2022), *Shaping the Future of E2R Validators and Facilitators*, in D. Dejica, Ó. García Muñoz, S. Șimon et al. (eds.), "The Status of Training Programs for E2R Validators and Facilitators in Europe", Esedra, 2022

Ó. García Muñoz (2012), *Lectura fácil: Métodos de redacción y evaluación*, Centro Español de Documentación sobre Discapacidad (CEDD), 2012

K. Gerhalter (2024), *How do DeepL and ChatGPT process information structure and pragmatics? An exploratory case study on topicalized infinitives in Spanish (and Portuguese)*, in "AI-Linguistica. Linguistic Studies on AI-Generated Texts and Discourses", vol. 1, 2024, n. 1

S. Hansen-Schirra, S. Gutermuth (2018), *Modellierung und Messung Einfacher und Leichter Sprache*, in S. Jekat, M. Kappus, K. Schubert (Hrsg.) "Barrieren abbauen, Sprache gestalten", Working Papers of Applied Linguistics 14, 2018

S. Hansen-Schirra, J. Nitzke, S. Gutermuth et al. (2020), *Technologies for translation of specialised texts into easy language*, in S. Hansen-Schirra, C. Maaß (eds.), "Easy Language Research: Text and User Perspectives", Frank & Timme, 2020

A.R. Kaplan (2021), *Suitability of Neural Machine Translation for Producing Linguistically Accessible Texts. Exploring the Effects of Pre-Editing on Easy-to-Read Administrative Documents*, Manuscript of the PhD thesis, University of Geneva, 2021

J. Kercher (2013), *Verstehen und Verständlichkeit von Politikersprache. Verbale Bedeutungsvermittlung zwischen Politikern und Bürgern*, Springer, 2013

T. Kopp, A. Rempel, A. Schmidt, M. Spieß (2023), *Towards machine translation into Easy Language in public administrations: Algorithmic alignment suggestions for building a translation memory*, in S. Deilen, S. Hansen-Schirra, S. Hernández Garrido et al. (eds.) "Emerging Fields in Easy Language and Accessible Communication Research", Frank & Timme, 2023

J. Kröger, C. Maaß (2024), *Mangelnde Verständlichkeit durch Fachsprache in Gesundheitsinformationen zu chronischen Erkrankungen – eine qualitative Korpusanalyse*, in "Prävention und Gesundheitsförderung", vol. 19, 2024

K. Lang (2024), *The legal situation of accessible communication in Germany*, in C. Maaß, I. Rink (eds.), "Handbook of Accessible Communication", Frank & Timme, 2024

K. Lang (2021), *Auffindbarkeit, Wahrnehmbarkeit, Akzeptabilität. Webseiten von Behörden*, in "Leichter Sprache vor dem Hintergrund der rechtlichen Lage", Frank & Timme, 2021

K. Lang (2019), *Die rechtliche Lage zu Barrierefreier Kommunikation in Deutschland*, in C. Maaß, I. Rink (eds.) "Handbuch Barrierefreie Kommunikation", Frank & Timme, 2019

C. Lindholm, U. Vanhatalo (2021), *Handbook of Easy Languages in Europe*, Frank & Timme, 2021

C. Maaß (2024-a), *Intralingual Translation in Easy Language and in Plain Language*, in L. Pillière, Ö. Berk Albachten (eds.), "The Routledge Handbook of Intralingual Translation", Routledge, 2024

C. Maaß (2024-b), *Hi ChatGPT, translate this text into Easy Language. Is the new Easy Language translator a machine?*, in "Proceedings of the XLIV International VAKKI Symposium", University of Vaasa, 2024

C. Maaß (2020), *Easy language – Plain Language – Easy Language Plus. Balancing comprehensibility and acceptability*, Frank&Timme, 2020

C. Maaß (2015), *Leichte Sprache. Das Regelbuch*, Lit., 2015

C. Maaß, C. Fioravanti (2025), *Translating Easy Language administrative texts: a quantitative analysis of DeepL's performance from German into Italian using a bilingual corpus*, forthcoming

C. Maaß, L.M. Maaß (2024), *Leichte Sprache bei intellektuellen Beeinträchtigungen*, in "Sprache – Stimme – Gehör", vol. 48, 2024, n. 4

C. Maaß, I. Rink (2021), *Translating Legal Texts into Easy Language*, in C. Fioravanti (ed.) "Communicating the law and public information to vulnerable audiences", "JOAL", vol. 9, 2021, n. 1, special issue

C. Maaß, I. Rink, S. Hansen-Schirra (2021), *Easy Language in Germany*, in C. Lindholm, U. Vanhatalo (eds.), "Handbook of Easy Languages in Europe", Frank & Timme, 2021

C. Maaß, I. Rink, C. Zehrer (2014), *Leichte Sprache in der Sprach- und Übersetzungswissenschaft*, in S.J. Jekat, H.E. Jüngst, K. Schubert, C. Villiger (Hg.), "Sprache barrierefrei gestalten. Perspektiven aus der Angewandten Linguistik", Frank & Timme, 2014

C. Maaß, L.M. Schwengber (2022), *Easy Language and Plain Language in Germany*, in "Rivista internazionale di tecnica della traduzione / International Journal of Translation", 2022, n. 24

L.M. Maaß (2023), *Accessibility on Social Media: A Corpus Driven Analysis of Official German Websites (Aktion Mensch, German Federal Government)*, in S. Deilen, S. Hansen-Schirra, S. Hernández Garrido et al. (eds.) "Emerging Fields in Easy Language and Accessible Communication Research", Frank & Timme, 2023

M. Magris (2022), *Il linguaggio facile da leggere e da capire in Alto Adige*, Treccani, 2022

D. Melchiori, S. Siemons (2024), *Possibilities and limits in translating texts into Easy Language: dealing with multilingual texts in the context of accessible communication*, Workshop at ÖLT 2024, Innsbruck, 17 December 2024

M. Miliani, F. Alva-Manchego, A. Lenci (2023), *Simplifying Administrative Texts for Italian L2 Readers with Controllable Transformers Models: A Data-driven Approach*, in F. Boschetti, G.E. Lebani, B. Magnini, N. Novielli (eds.), "CLiC-it 2023 – Proceedings of the 9th Italian Conference on Computational Linguistics", 2023

J. Nitzke, S. Hansen-Schirra (2021), *A short guide to post-editing*, Language Science Press, 2021

D. Nozza, G. Attanasio (2023), *Is It Really That Simple? Prompting Language Models for Automatic Text Simplification in Italian*, in F. Boschetti, G.E. Lebani, B. Magnini, N. Novielli (eds.), "CLiC-it 2023 – Proceedings of the 9th Italian Conference on Computational Linguistics", 2023

E. Perego (2021), *Easy Language in Italy*, in C. Lindholm, U. Vanhatalo (eds.), "Handbook of Easy Languages in Europe", 2021

M.E. Piemontese (1996), *Capire e farsi capire: teorie e tecniche della scrittura controllata*, Tecnodid, 1996

A.A. Rescigno, J. Monti (2023), *Gender Bias in Machine Translation: a statistical evaluation of Google Translate and DeepL for English, Italian and German*, in C. Orăsan, R. Mitkov, G. Corpas Pastor, J. Monti (eds.), "International Conference on Human-Informed Translation and Interpreting Technology (HiT-IT 2023)"

I. Rink (2024), Communication Barriers, in C. Maaß, I. Rink (eds.), "Handbook of Accessible Communication", Frank & Timme, 2024

I. Rink (2020), *Rechtskommunikation und Barrierefreiheit. Zur Übersetzung juristischer Informations- und Interaktionstexte,* in "Leichte Sprache", Frank & Timme, 2020

M. Russodivito, V. Ganfi, G. Fiorentino, R. Oliveto (2024), *AI vs. Human: Effectiveness of LLMs in Simplifying Italian Administrative Documents*, in F. Dell'Orletta, A. Lenci, S. Montemagni, R. Sprugnoli (eds.), "CLiC-it 2024 – Proceedings of the 10th Italian Conference on Computational Linguistics", 2024

M. Ryan, T. Naous, W. Xu (2023), *Revisiting non-English Text Simplification: A Unified Multilingual Benchmark*, in A. Rogers, J. Boyd-Graber, N. Okazaki (eds.), "Proceedings of the 61st Annual Meeting

of the Association for Computational Linguistics (Volume 1: Long Papers)", Association for Computational Linguistics, 2023

I. Schiffler (2022), *Das Prüfen auf dem Prüfstand: Die Rolle der Moderatorinnen beim Prüfen von Texten*, in "Leichter Sprache", Frank & Timme, 2022

R. Schulz, K. Czerner-Nicolas, J. Kegenhardt (2020), *Easy Language Interpreting*, in S. Hansen-Schirra, C. Maaß (eds.), "Easy Language Research: Text and User Perspectives", Frank & Timme, 2020

F.C. Sciumbata (2022), *Manuale dell'Italiano facile da leggere e da capire*, Franco Cesati editore, 2022

F.C. Sciumbata (2021), *Dal Plain Language all'Easy-To-Read per i lettori con disabilità intelletive: oltre la semplificazione*, in "Lingue e Linguaggi", vol. 41, 2021

N. Spring, M. Kostrzewa, D. Fröhlich et al. (2023), *Analyzing sentence alignment for automatic simplification of German texts*, in S. Deilen, S. Hansen-Schirra, S. Hernández Garrido et al. (eds.) "Emerging Fields in Easy Language and Accessible Communication Research", Frank & Timme, 2023

S. Štajner, M. Franco-Salvador, P. Rosso, S.P. Ponzetto (2018), *CATS: A Tool for Customized Alignment of Text Simplification Corpora*, in N. Calzolari, K. Choukri, C. Cieri et al. (eds.), "Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)", European Language Resources Association (ELRA), 2018

M. Tavosanis (2019), *Valutazione umana di Google Traduttore e DeepL per le traduzioni di testi giornalistici dall'inglese verso l'italiano*, in R. Bernardi, R. Navigli, G. Semeraro (eds.), "CLiC-it 2019 – Proceedings of the Sixth Italian Conference on Computational Linguistics", 2019

E. Wiesmann (2019), *Machine Translation in the Field of Law: A Study of the Translation of Italian Legal Texts into German*, in "Comparative Legilinguistics", vol. 37, 2019, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0219 • articolo sottoposto a peer review • pubblicato in anteprima l'11 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Veronica Montozzi

Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza

Il valore economico e il conseguente rilievo assunto dai dati nell'ambito del mercato hanno determinato lo sviluppo di una nuova forma di capitalismo che comporta il rischio di realizzare un ordine economico che tende a comprimere i diritti fondamentali, creando nuove forme di disuguaglianza, e che rischia di alterare i meccanismi concorrenziali del mercato, con l'affermarsi del dominio dei c.d. poteri privati digitali. Partendo dall'analisi del fenomeno della monetizzazione dei dati, il contributo mira ad esaminare il recente approccio normativo dell'Unione europea che, nel fornire risposta alle sfide poste dallo sviluppo della *data driven economy*, tenta di delineare un modello di regolazione dei dati e delle nuove tecnologie che tenga in considerazione, da un lato, l'interesse economico relativo allo sviluppo di un mercato digitale europeo; dall'altro, quello di tutelare i diritti e le libertà fondamentali degli individui, adottando, sulla scia del nuovo movimento del costituzionalismo digitale, una serie di provvedimenti tramite i quali reinterpretare e riequilibrare il quadro dei poteri e delle libertà che vengono in rilievo. L'articolo riflette, dunque, sulle criticità derivanti dalla commistione delle diverse discipline che intervengono nelle vicende emergenti nell'ecosistema digitale, *in primis* la tutela della protezione dei dati e quella della concorrenza, analizzando le recenti pronunce giurisprudenziali che hanno tentato di individuare soluzioni per i casi concreti.

Protezione dei dati – Concorrenza – Monetizzazione dei dati – Poteri privati digitali – Costituzionalismo digitale

The new challenges of data regulation: analysis of a model starting from the intersection between personal data protection and competition

The economic value and the consequent importance assumed by data in the context of the market have led to the development of a new form of capitalism that involves the risk of creating an economic order that tends to compress fundamental rights, creating new forms of inequality, and which risks altering the competitive mechanisms of the market, with the affirmation of the domination of the so-called digital private powers. Starting from the analysis of the phenomenon of data monetization, the paper aims to examine the recent regulatory approach of the European Union which, in responding to the challenges posed by the development of the data-driven economy, attempts to outline a model of regulation of data and new technologies that takes into account, on the one hand, the economic interest related to the development of a European digital market; on the other hand, that of protecting the fundamental rights and freedoms of individuals, adopting, in the wake of the new movement of digital constitutionalism, a series of measures through which to reinterpret and rebalance the framework of powers and freedoms that come to the relief. The article reflects, therefore, on the critical issues deriving from the mixture of the different disciplines that intervene in the emerging events in the digital ecosystem, first and foremost the protection of personal data and of competition, analyzing the recent case law that have attempted to identify solutions for concrete cases.

Data protection – Competition – Data monetisation – Digital private powers – Digital constitutionalism

L'Autrice è dottoranda di ricerca in Discipline giuridiche pubblicistiche, curriculum Discipline pubblicistiche, internazionalistiche ed europee presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre

Sommario: 1. Circolazione dei dati, protezione dei dati e concorrenza: la sfida del nuovo costituzionalismo digitale. – 2. Profili problematici della c.d. monetizzazione dei dati personali. – 3. Il caso Facebook tra Italia e Germania. – 4. La decisione della Corte di giustizia: la necessaria cooperazione delle autorità amministrative indipendenti. – 5. Il Consiglio di Stato riafferma il principio leale collaborazione. – 6. Conclusioni.

1. Circolazione dei dati, protezione dei dati e concorrenza: la sfida del nuovo costituzionalismo digitale

La circolazione dei dati è la chiave di volta dell'economia digitale, settore chiave nella competizione economica globale. Già dal titolo del Regolamento UE 2016/679[1], infatti, si evince come, accanto alla tutela della protezione dei dati, una delle principali esigenze dell'Unione europea sia quella di promuovere la libera circolazione di essi in armonia con la tutela della persona, mediante regole che impediscano al fenomeno circolatorio di spingersi oltre il limite della dignità della persona[2], "nell'ottica di favorire un clima di fiducia per lo sviluppo di un'economia digitale nel mercato interno"[3]. Come preannunciato dal professore Thomas W. Malone nel 1987[4], nell'era dell'informazione, del digitale, delle nuove tecnologie, infatti la centralità assunta dai dati personali nella società, sempre più *data driven* e caratterizzata dalla crescente applicazione dell'IoT e dell'Intelligenza Artificiale, insieme alla loro attrazione entro una logica di consumo e di scambio[5], ha determinato il diffondersi, accanto all'economia tradizionale, della c.d. *data driven economy*, ossia un'economia basata sui dati e sulla loro attitudine ad incrementare le opportunità di business. Nei mercati "*data rich*", i dati hanno quindi assunto un rilevante valore economico[6], tanto da esser definiti il nuovo "petrolio"[7],

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
2. In senso critico Gentili 2022, in cui l'A. osserva che "a guardar bene non c'è un vero bilanciamento. C'è piuttosto una prioritaria legittimazione del mercato dei dati, con pochi, fiacchi e platonici limiti a protezione della persona".
3. Calisai 2019, p. 327 ss.
4. Cfr. Malone–Yates–Benjamin 1987, in cui Malone aveva previsto l'avvento dei "mercati elettronici".
5. "La presenza di IA è ormai una realtà acquisita ed in sviluppo esponenziale nel panorama industriale mondiale", Naldi 2018, p. 225-238. In questo scritto l'A. compie un'accurata analisi circa lo stato degli investimenti in IA, soprattutto da parte dei "cinque giganti del web", ossia Google, Apple, Facebook, Microsoft e Amazon.
6. Sul valore commerciale dei dati personali approfondiscono *ex multis*: Cremona–Laviola–Pagnanelli 2022; Battelli 2022, pp. 355-364; Resta 2019, pp. 127-153; Malgieri–Custers 2018; Midiri 2016, pp. 355-373.
7. Così *The world's most valuable resource is no longer oil, but data*, in "The economist", 6 maggio 2017; sul punto anche Colapietro 2021, p. 834: "Come il carbone e la macchina a vapore hanno rappresentato gli elementi essenziali della Prima rivoluzione industriale e il petrolio e il motore a scoppio quelli della Seconda rivoluzione industriale, i dati gli algoritmi e l'Intelligenza artificiale rappresentano i fondamenti di quella che stiamo vivendo noi e che oggi è ancora nella sua fase iniziale".

in quanto sempre più utilizzati nelle strategie imprenditoriali e rappresentando anche la fonte di un rilevante vantaggio competitivo[8]. Tuttavia, in tale contesto, caratterizzato da asimmetrie strutturali e funzionali[9], i dati vengono sfruttati per finalità commerciali, spesso a insaputa dello stesso utente, e l'enorme disponibilità delle informazioni – nonché la concentrazione delle stesse nelle mani di pochi – ha determinato l'erompere di nuovi poteri[10], i "poteri privati digitali"[11], che dettano le regole del gioco, sviluppando poteri sempre più simili ai poteri pubblici[12] e creando monopoli difficili da scardinare.

Questi sviluppi mettono in crisi le tradizionali forme di regolazione giuridica, dell'azione antitrust e della protezione dei dati personali[13], in quella che sembra delinearsi come una nuova forma di capitalismo – definito "capitalismo della sorveglianza"[14] – in cui cambiano, come detto, le regole del gioco e le dinamiche di domanda ed offerta funzionali ad assicurare la democrazia del mercato[15].

È innegabile infatti come nell'industria 4.0, caratterizzata dall'accumulo massivo di grandi quantità di informazioni personali da parte delle imprese, nonché, come vedremo, dalla continua ricerca di strategie per raccogliere dati, quali i *dark patterns*[16] o il c.d. *paywall*, si annidi il rischio di realizzare un ordine economico che tende a comprimere i diritti fondamentali associati all'autonomia individuale, creando nuove forme di disuguaglianza, e di alterare i meccanismi concorrenziali del mercato, rendendo necessario che l'attenzione venga spostata sulle tutele da accordarsi all'utente nell'ottica di rafforzarne la posizione quale soggetto debole nel contesto digitale e riequilibrare le asimmetrie di potere esistenti tra parti diverse del contratto[17].

È nell'ottica di implementare la tutela dei diritti che si pone il movimento del nuovo costituzionalismo digitale[18]: esso si prefigge l'obiettivo di introdurre strumenti che apprestino un'adeguata difesa dei diritti nel rapporto con i nuovi poteri, nella consapevolezza che le dimensioni assunte dal nuovo fenomeno digitale necessitano della massima attenzione da parte delle istituzioni politiche e regolatorie[19]. In questa direzione si sta

8. Cfr. Resta 2019, p. 127; v. anche Solinas 2021, p. 323: "Il rilievo da cui partire è che i dati personali sono ormai considerati una riserva economica a tutti gli effetti".
9. Di asimmetrie "strutturali e funzionali dei rapporti giuridici online" parla Cremona 2021, pp. 681-696; v. anche Simoncini 2019, pp. 63-89.
10. Espressione coniata da Predieri 1997.
11. Si rinvia a Simoncini–Cremona 2021, pp. 244-260.; Cfr. Pollicino 2019; Pollicino 2019-a; Mezzanotte 2018, pp. 507-530.
12. Klonick 2018; sul punto si v. anche Cremona 2021, p. 686, il quale spiega che "I nuovi sovrani […] i padroni degli algoritmi più intelligenti del mondo pervadono i mercati e avocano a sé sempre maggiori funzioni, anche tradizionalmente proprie dei pubblici poteri".
13. Midiri 2020.
14. Zuboff 2019.
15. Così osserva Sartoretti 2019.
16. Con tale termine si fa riferimento a tecniche che utilizzano la psicologia per convincere gli utenti a cedere i propri dati o a prestare il consenso al trattamento. Sul punto v. Mursia–Trovato 2021, pp.165-189.
17. Sul punto v. Iannuzzi 2024, p. 111, il quale evidenzia che "In un sistema senza intermediari il singolo si è mostrato spesso in balìa dei giganti della rete, per via dello sbilanciamento delle posizioni e della notevole asimmetria informativa"; v. anche Caggia 2019, p. 260.
18. Sul punto Cheli 2021, p. 955, prende atto che la rivoluzione industriale, messa in atto dalla digitalizzazione – più precisamente per effetto diretto "delle trasformazioni che la scienza e la tecnica hanno determinato e stanno determinando nella sfera fisica, psichica e relazionale della persona umana" – apre la strada ad una "nuova stagione del costituzionalismo" che denomina stagione del "costituzionalismo digitale". Secondo l'A. "questa nuova forma di costituzionalismo mira ad ampliare, a completare e a rafforzare gli strumenti del costituzionalismo tradizionale".
19. Cremona 2021, p. 689.

muovendo il legislatore europeo che, nel tentativo di attuare una più efficace ed efficiente definizione delle regole dei meccanismi propri di questa nuova forma di capitalismo[20], ha ritenuto opportuno recuperare la centralità delle fonti[21], optando per strumenti di *hard law*, sostanziatisi nei regolamenti recentemente approvati, quali il Digital Markets Act (DMA), il Digital Services Act (DSA), il Data Act (DA) e il Data Governance Act (DGA), insieme al Regolamento sull'IA. Tali provvedimenti si inseriscono nel più ampio progetto normativo dell'Unione europea di divenire il leader all'interno del mercato mondiale dei dati e delle tecnologie digitali, per il raggiungimento del quale un ruolo fondamentale è svolto dalla libera circolazione dei dati[22]. Pertanto, i nuovi Regolamenti mirano a definire, nel loro insieme e in combinato disposto col GDPR, un nuovo modello europeo di regolazione dei dati, tramite il quale il legislatore europeo, tenuta a mente la pluralità di interessi coinvolti, tenta di trovare un nuovo punto di equilibrio tra la tutela dei valori della persona e le esigenze di mercato, incentivando da un lato la circolazione dei dati, al fine di stimolare un mercato unico europeo, che prenda atto del valore economico dei dati, e dall'altro, aumentando il controllo pubblico sulle dinamiche emergenti nell'ecosistema digitale, in modo da realizzare una correzione del mercato in senso conforme non solo ai diritti fondamentali dell'individuo[23], ma anche alle esigenze degli imprenditori e delle PMI[24].

In tale quadro, volto a incardinare in schemi regolatori una realtà in costante e profondo mutamento, assumono un ruolo significativo le autorità amministrative indipendenti[25], le quali, in vista dei poteri di vigilanza e sanzionatori di cui sono investiti, sono chiamate a ricoprire un ruolo di crescente protagonismo nella difesa delle libertà e dei diritti di tutti gli attori coinvolti sia a livello europeo che nazionale[26]. Per tale motivo, i nuovi provvedimenti, prevedono infatti l'implementazione e l'integrazione del lavoro delle *authorities*, soprattutto nell'ambito delle dinamiche concorrenziali nei mercati digitali. Tuttavia, le novità introdotte dai nuovi regolamenti europei e il nuovo ruolo assunto dai dati presentano il rischio di sovrapposizioni delle funzioni attribuite a ciascuna autorità e alimentano, di fatto, la difficoltà di comprendere chi sia competente a risolvere le questioni emergenti nell'ecosistema digitale, rappresentando un serio problema specie per le imprese, che si ritrovano gravate di una serie di obblighi giuridici provenienti da fonti diverse, il cui inadempimento può attivare l'azione di autorità diverse, con conseguenze sanzionatorie di diverso genere.

20. Sartoretti 2019, p. 5.
21. V. anche Iannuzzi 2021, pp. 31-51, il quale individua quale nuova funzione del costituzionalismo, quella di "operare anche nella direzione di limite all'abnorme potere di soggetti privati che esercitano ormai sul web poteri paracostituzionali".
22. Parlamento europeo, *Risoluzione del Parlamento europeo su una strategia europea per i dati (2020/2217(INI))*, 25 marzo 2021.
23. *Ivi*, p.to 9, il Parlamento europeo "ritiene che l'Unione debba adoperarsi per una governance dei dati a livello dell'UE e per una società e un'economia dei dati antropocentriche, basate sui valori dell'Unione del rispetto della vita privata, della trasparenza e del rispetto dei diritti e delle libertà fondamentali, in cui i cittadini siano in grado di prendere decisioni informate in merito ai dati che generano o che li riguardano".
24. Cfr. Iannuzzi 2024, p. 108, il quale evidenzia che le piccole e medie imprese (PMI) "rappresentano la specificità europea nel mercato delle tecnologie e dell'informazione delle telecomunicazioni (ICT), e non solo, e che rischiano di rimanere schiacciate nella contesta globale, dal potere dei giganti della tecnologia (big tech)".
25. Sull'importanza dell'azione delle autorità amministrative indipendenti Cheli 2021, p. 956, scrive: "è certo che un ruolo rilevante potrà essere svolto da queste autorità, in ragione della loro nascita e della loro ragione di essere come soggetti 'bifronte' ancorati sia allo spazio nazionale che a quello europeo. […] Le autorità amministrative indipendenti […] sono anche soggetti che esercitano un potere qualitativamente diverso dai poteri tradizionali dello Stato, potere dove si combinano le tradizionali funzioni dello Stato al fine di offrire uno strumento rapido, flessibile e tecnicamente attrezzato per la difesa dei diritti nel rapporto con i nuovi poteri".
26. Cfr. Simoncini 2021, pp. 723-732; sul punto v. anche Calzolaio 2024, pp. 84-106.

Nei paragrafi che seguono, si cercherà di mostrare il dispiegarsi nella pratica di tale fenomeno, partendo da un approfondimento sul tema della c.d. monetizzazione dei dati personali, e le conseguenti criticità, e analizzando le vicende giurisprudenziali che ne sono derivate e che hanno dato piena dimostrazione degli effetti di questo intreccio di normative e di competenze delle autorità indipendenti.

2. Profili problematici della c.d. monetizzazione dei dati personali

Dall'analisi delle abitudini del mercato, si evince la circostanza che la raccolta di dati personali "è sempre più il motivo che anima l'impresa"[27]. La ragione per cui i dati personali hanno attirato l'attenzione delle imprese, venendo collocati alla base del loro modello di business, riguarda il fatto che i dati possono essere "trattati, analizzati, arricchiti e quindi riutilizzati al fine di trarne informazioni suscettibili di rilievo economico"[28], rendendo evidente come, tramite il loro trattamento, i dati vengano "patrimonializzati", traendone direttamente utilità economica o estraendone informazioni in seguito scambiabili sui mercati digitali[29].

Tra i vari *business models* sviluppatisi nella prassi del mercato[30], la fattispecie più comune nelle imprese, specie quelle che dispongono di *digital platforms*, è il modello c.d. *zero-price*[31]. Tale modello si basa sulla fornitura di servizi o contenuti digitali all'utente, che viene effettuata senza che quest'ultimo debba eseguire una controprestazione di natura pecuniaria. In cambio della fruizione di servizi/contenuti offerti, però, l'utente deve prestare il proprio consenso al trattamento dei propri dati personali per finalità che spaziano dalla necessità di eseguire la prestazione richiesta fino al soddisfacimento di interessi commerciali[32]. Così come configurata, in tale operazione i dati personali si pongono come corrispettivo per la fornitura di contenuti o servizi digitali[33]. Ciò ha condotto parte della dottrina a considerare la fornitura di dati personali alla stregua di una controprestazione, da cui si ricava l'equiparazione dei dati

27. Il tema è stato oggetto di un esame congiunto svolto dall'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali, nell'*Indagine conoscitiva sui big data*, 10 febbraio 2020.
28. D'Ippolito 2022, p. 58. Sul punto si veda anche Stazi–Corrado 2019, p. 471, dove si afferma che "la medesima dottrina ha rilevato come nell'ecosistema dell'economia digitale i dati personali siano tipicamente utilizzati proprio per finalità ulteriori, come la profilazione e la pubblicità mirata, costituendo in tal senso il 'corrispettivo' per l'accesso al servizio".
29. Zeno-Zencovich 2019, pp. 22-38. Sul punto la stessa AgCom, *Osservatorio sulle piattaforme online*, 27 dicembre 2019, p. 23, osserva che: "La disponibilità di grandi masse di dati individuali consente alle piattaforme di compiere un'accurata profilazione degli utenti, dalla quale dipende la possibilità per gli inserzionisti che si servono delle piattaforme di raggiungere target specifici di consumatori". Dall'analisi svolta dall'AgCom si ricava che per Facebook la pubblicità online, ottenuta mediante il trattamento dei dati forniti dagli utenti e la successiva vendita, genera il 99% dei ricavi, mentre per Google la raccolta pubblicitaria rappresenta ben l'85% degli introiti complessivi.
30. Ci si riferisce ai tre principali modelli di *business* incentrati sul trattamento dei dati, ossia: *zero-price, personal data economy, pay for privacy*. Per un approfondimento sul punto v. Elvy 2017, pp. 1369-1454. Si v. anche Ricciuto 2020, in cui l'A. evidenzia come lo schema dei modelli negoziali dei dati sia infatti aperto a diverse formulazioni.
31. Si tratta del modello di business che viene applicato principalmente da imprese quali Facebook, Google, Twitter come evidenziato da Competition and Markets Authority (CMA), *The commercial use of consumer data - Report on the CMA's call for information*, giugno 2015.
32. In senso critico si v. Strandburg 2013, pp. 96–99. L'A. ammonisce, infatti, l'utilizzo dell'etichetta *zero-price model* – definito anche *data-as-payment model* – dal momento che "Internet users do not know the 'prices' they are paying for products and services […] because they cannot reasonably estimate the marginal disutility that particular instances of data collection impose on them".
33. Ricciuto–Solinas 2021.

personali alla moneta e la massima che afferma che "se il servizio è gratuito vuol dire che la merce è l'utente", ossia la c.d. *Internet cost trap*[34].

Occorre, dunque, procedere ad un mutamento di prospettiva che giunga a valorizzare, nel necessario bilanciamento con i diritti fondamentali della persona, anche i profili di carattere patrimoniale del trattamento, propri dell'economia dei dati profilati[35], nella quale l'informazione relativa alla persona diventa essa stessa oggetto di scambio.

A lungo, infatti, il trattamento dei dati, quali elementi costitutivi della personalità dell'individuo, è stato associato ad un diritto alla privacy riconosciuto in un contesto più attento al riconoscimento dei diritti della persona che alla definizione di regole volte a disciplinare il nascente mercato dei dati – c.d. *Data Market* – all'interno del quale, invece, i dati si presentano quale principale risorsa economica di una società, come quella attuale, fondata sulle informazioni[36].

In ragione della stretta inerenza che vi è tra l'informazione e la persona, in grado di delinearne l'identità personale e influenzarne le condizioni di vita[37], la disciplina in materia di tutela dei dati personali è però sempre stata ancorata alla tutela della persona, ricomprendendo l'intervento normativo europeo nell'alveo della disciplina dei diritti fondamentali della persona[38]. Qualificando il diritto alla protezione dei dati personali come diritto fondamentale, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea, esso non potrebbe costituire oggetto di atti di disposizione e per questo non sarebbe immaginabile un'attività contrattuale avente a oggetto lo stesso[39]. Accanto alla indisponibilità, la situazione giuridica soggettiva coinvolta si caratterizza anche per la necessarietà, l'irrinunciabilità, l'intrasmissibilità e l'imprescrittibilità[40], attribuendo al titolare la possibilità di pretendere che i dati siano trattati da terzi solo nel rispetto delle regole stabilite dalla legge.

Tuttavia, la realtà fattuale si presenta in contrasto con la ricostruzione appena prospettata della situazione giuridica. È evidente, infatti, che la digitalizzazione ha invece dato vita ad un'economia digitale, nell'ambito della quale le imprese possono sfruttare l'enorme quantità di informazioni ricavabili dai dati per promuovere nuovi prodotti e servizi, dando vita alla c.d. *Data Driven Innovation*[41].

Il carattere pervasivo delle logiche del mercato ha messo, quindi, in dubbio l'utilizzabilità dei diritti della personalità mediante l'attribuzione di poteri di disposizione sugli stessi. È stato notato, infatti, che "la commercializzazione dei dati personali si distingue solo in parte dalla commercializzazione di altri diritti della personalità come, ad esempio, il diritto all'immagine"[42]. È ormai da

34. Ci si riferisce alla "trappola del dono", di cui discorre De Franceschi 2019, p. 1386.
35. Nicita 2019, p. 1164, il quale descrive il dato profilato come "un caso particolare di informazione che viene appropriata dalla piattaforma che lo profila, spesso attraverso scambi impliciti".
36. Battelli 2022; Ricciuto 2020, p. 642, per il quale, pur avendo la Dir. 95/46/CE creato le condizioni per la circolazione del dato personale al pari di altri beni e servizi nel contesto economico e sociale europeo, resta sullo sfondo la questione della regolazione della circolazione dei dati, quale elemento alla base dell'economia e della realtà sociale contemporanea.
37. D'Ippolito 2022.
38. Ricciuto 2020.
39. "Al pari degli altri attributi della persona […], non veniva concepita nessuna possibilità di vendita o redditività del dato personale" (Ricciuto 2018, p. 698).
40. Sulla categoria si rinvia a De Cupis 1982, p. 283.
41. Il concetto fa riferimento, in sostanza, alla capacità delle imprese e degli organismi pubblici di acquisire le informazioni derivanti dal trattamento dei dati e piegarle ai propri scopi, come prendere decisioni consapevoli o sviluppare servizi e prodotti migliori. L'OCSE, infatti, fornisce la definizione di *Data Driven Innovation* come la tendenza per cui "techniques and technologies for processing and analysing large volumes of data, which are commonly known as 'big data', are becoming an important resource that can lead to new knowledge, drive value creation, and foster new products, processes, and markets". (*Data-driven Innovation for Growth and Well-being: Interim Synthesis Report*, ottobre 2014, p. 4.).
42. De Franceschi 2019, p. 1381.

tempo, infatti, che nel panorama giuridico si sono fatte spazio fattispecie contrattuali aventi ad oggetto "beni personali", le quali sono state oggetto di un processo di tipizzazione sociale che è stato poi attratto nell'alveo degli interessi meritevoli di tutela per l'ordinamento giuridico *ex* art. 1322 c.c.[43] È da notare che la componente patrimoniale emerge anche in operazioni in cui si riscontra la gratuità per la mancanza di una controprestazione pecuniaria, ma che in realtà realizzano un vantaggio economico anche a fronte della cessione di un proprio bene personale.

Tale processo di mercificazione ha interessato – si ribadisce – pure i dati personali, imponendo al legislatore comunitario una "scelta precisa", consistente nel mantenere l'originaria impostazione delle normative nazionali e degli accordi internazionali, o di sostituirla con una disciplina che sancisca apertamente la mercificazione dei dati e regoli la circolazione di tale bene[44].

La questione del valore di scambio dei dati contro prodotti e servizi, in assenza di una disciplina specifica che si occupa della circolazione dei dati su "base contrattuale", ha reso necessaria una riflessione da cui sono scaturiti due principali orientamenti.

Un primo indirizzo nega la natura di bene economico ai dati personali, e pertanto, ravvisa, in ogni ipotesi di trattamento dei dati, la presenza di una responsabilità da fatto illecito resa inoperante dalla prestazione del consenso dell'avente diritto ovvero di un atto unilaterale di tipo autorizzatorio. Tale argomentazione si basa sull'impostazione volta a privilegiare il carattere non patrimoniale e indisponibile dei diritti della personalità, i quali, non essendo per definizione trasferibili a terzi, restano connessi al soggetto che ne è titolare. Il vantaggio di tale impostazione consiste nella salvaguardia delle prerogative riconosciute in capo al soggetto consenziente, lasciando così inalterato il principio di indisponibilità dei diritti della personalità[45].

Una diversa lettura del fenomeno ha condotto la dottrina a sostenere la necessità di "reinventare il capitalismo"[46], orientandosi ad affermare il valore commerciale assunto dagli attributi della personalità, in particolare dai dati personali, tale da renderli assimilabili ai beni in senso giuridico e quindi autonomamente suscettibili di essere oggetto di disposizione mediante strumento contrattuale[47]. Questa lettura è coerente con il valore economico assunto dai dati e trova riscontro non solo nelle strategie imprenditoriali, ma anche nelle considerazioni effettuate sul punto da parte del legislatore comunitario[48]. Tuttavia, è stato osservato come la circostanza che le informazioni abbiano assunto una valenza economica, non sia di per sé un "presupposto condizionante rispetto alle

43. Cfr. art. 1322, co 2 c.c.: "Le parti possono anche concludere contratti che non appartengono ai tipi aventi una disciplina particolare, purché siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico". Un esempio in questo senso è rappresentato dal contratto di sponsorizzazione sportiva, con il quale viene concesso l'utilizzo della propria immagine, verso il pagamento di un prezzo o altra prestazione non pecuniaria.
44. Simitis 1997, p. 575.
45. In favore dell'indisponibilità del diritto alla protezione dei dati personali si evidenzia la posizione del Garante europeo per la protezione dei dati personali, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts or the supply of digital content*, 14 marzo 2017, il quale afferma che i dati non possono essere considerati alla stregua di una merce. Sullo stesso punto, in dottrina, Mirabelli 1993, pp. 313-330, secondo cui il consenso va inquadrato nella generale categoria di consenso dell'avente diritto che elimina l'antigiuridicità del comportamento. In senso contrario alla ricostruzione del consenso come "scriminante" si esprime Sica 2001, p. 630: "La categoria del consenso legittimante, sotto forma dell'ipotesi codificata dall'art. 50 c.p., non è, pertanto, calzante del tutto, probabilmente perché è carente, nel caso che ci occupa, il *prius* della 'titolarità del diritto', nel senso conseguente della libera, totale disponibilità del bene 'riservatezza'".
46. Mayer-Schönberger–Ramge, 2018.
47. Così Resta–Zeno-Zencovich 2018, pp. 411-440; Stazi–Corrado 2019; Resta 2019; Resta 2010, p. 38.
48. Cfr. Proposta di direttiva del Parlamento europeo e del Consiglio, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, Bruxelles, 9 dicembre 2015, COM(2015) 634.

scelte di valorazione giuridica dei beni"[49]. A ciò si aggiunga la considerazione che i dati sono delle entità immateriali, e in quanto tali risulta pertanto difficile applicare ad essi il modello proprietario tradizionale, che si incentra sul bene quale cosa materiale, che può costituire oggetto di diritti e che circola mediante contratto[50].

In realtà, occorre notare che il Regolamento UE 2016/679 prende atto, quanto meno in parte, del processo di *commodification* che ha interessato i dati personali, ed infatti – come osservato nel precedente paragrafo – la principale esigenza cui è indirizzata la disciplina in esso contenuta riguarda la libera circolazione dei dati, rendendosi evidente, infatti, come lo stesso concetto di circolazione dei dati personali rimandi all'idea di negoziabilità degli stessi[51].

In continuità con il GDPR, il legislatore europeo ha successivamente emanato, il 20 maggio del 2019, la Direttiva 2019/770/UE relativa a determinati aspetti dei contrati di fornitura di contenuto digitale e di servizi digitali. Essa si caratterizza per un approccio "giusrealistico"[52], che non ignora l'evoluzione dei rapporti di mercato e il valore assunto dai dati nell'economia dell'informazione, riconoscendo espressamente, per la prima volta, il processo di patrimonializzazione dei dati personali, attraverso la tipizzazione della fattispecie negoziale contenuti/servizi digitali verso dati personali, largamente diffusa nelle pratiche dell'ambiente digitale[53]. Tale fattispecie consiste nella fornitura onerosa di contenuti o servizi digitali[54] a fronte o del pagamento di un prezzo o della fornitura da parte di un soggetto dei propri dati, i quali, alla stregua del prezzo, integrano una controprestazione che si pone in rapporto di corrispettività con quella ricevuta.

La direttiva in questione muove dalla constatazione che nei c.d. *multi-sided markets*[55] la logica della gratuità nasconde una razionalità economica, nel senso che molti servizi, apparentemente gratuiti, in realtà vengono adeguatamente remunerati attraverso il flusso di dati personali che perviene a seguito dell'attivazione del servizio[56]. Tutto ciò è stato ulteriormente ribadito nella dir. 2019/2161/UE del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

Accogliendo una lettura c.d. *market oriented* del fenomeno, infatti, si è resa necessaria la previsione di una disciplina non divergente da quella

49. Resta 2019, il quale sottolinea che la scelta di stabilire se un'entità "sia un bene tecnicamente appropriabile e poi, secondariamente, se sia suscettibile di costituire oggetto di contratti" spetta in modo esclusivo all'ordinamento giuridico.
50. Stazi–Corrado 2019, p. 458.
51. Basunti 2020, p. 860 ss.
52. Resta 2019, p. 140.
53. Senigaglia 2020, p. 760 ss.
54. Cfr. considerando 19 della dir. 2019/770/UE, il quale ricomprende in tale categoria "programmi informatici, applicazioni, file video, file audio, file musicali, giochi digitali, libri elettronici o altre pubblicazioni elettroniche, nonché i servizi digitali che consentono la creazione, la trasformazione o l'archiviazione dei dati in formato digitale, nonché l'accesso a questi ultimi, fra cui i software come servizio quali la condivisione audio e video e altri tipi di *file hosting*, la videoscrittura o i giochi offerti nell'ambiente di *cloud computing* e nei media sociali".
55. I *multi-sided markets* si caratterizzano per il fatto di porre distinti gruppi di utenti in una situazione di interdipendenza reciproca. L'obiettivo della piattaforma che opera su due o più versanti è quello di attrarre più utenti su un versante, in modo tale che gli utenti sugli altri versanti si facciano carico dei costi necessari per interfacciarsi con il primo gruppo di utenti. Sul punto v. Commissione europea, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, 25 maggio 2016, COM (2016) 288.
56. Resta–Zeno-Zencovich 2018. Sul punto anche De Franceschi 2019, p. 1393. L'A. ritiene necessario un'evoluzione del concetto di "pagamento", al fine di ricomprendervi anche "l'esecuzione di una prestazione a carattere oneroso sotto forma del trasferimento e dell'autorizzazione al trattamento dei dati personali".

ordinaria, per quanto riguarda la tutela dei consumatori[57]. L'art. 3, par. 1 della Dir. 2019/770/UE, infatti, stabilisce l'applicabilità della direttiva sia ai contratti con cui un operatore economico fornisce, o si impegna a fornire, un bene o un servizio digitale dietro corrispettivo di un prezzo, sia ai contratti in cui "l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico"[58].

Il Garante europeo della protezione dei dati personali nel parere n. 4/2017 ha, però, puntualizzato che i diritti della personalità – nei quali rientra il diritto alla protezione dei dati personali – "non possono essere ridotti a semplici interessi dei consumatori", e che dunque i dati personali "non possono essere considerati una mera merce"[59]. Quest'indicazione è stata accolta dal legislatore europeo, il quale ha eliminato la parola "corrispettivo" dal testo finale della direttiva[60].

Da tali valutazioni è possibile cogliere il conflitto tra i due antitetici modelli di lettura del diritto alla protezione dei dati personali: da un lato, il modello improntato alla visione patrimonialistica, quale quello contenuto nella direttiva del 2019; dall'altro il modello costruito in chiave personalistica, delineato dal Garante, che rifiuta qualsiasi ricostruzione che possa concepire la fornitura di dati personali quale corrispettivo di prestazioni contrattuali. La presa di posizione del Garante si giustifica in ragione della specificità dei diritti della personalità, i quali nel momento in cui assumono valore economico devono essere necessariamente collocati su un piano diverso dagli altri beni, data la loro inerenza all'identità della persona[61]. Dal momento, quindi, che ogni forma di esplicazione della personalità individuale trova il limite della dignità umana, si rende necessario che il regime giuridico della circolazione dei beni personali, in particolare delle informazioni personali, tenga conto di tale assunto.

Non essendo, però, rintracciabile nella disciplina eurounitaria alcun divieto al fenomeno della commercializzazione dei dati personali – anzi, tale possibilità è ammessa e codificata[62] – occorre constatare, a discapito di quanto affermato dal Garante, che sia possibile concludere un contratto di fornitura di un servizio o contenuto digitale fornendo i propri dati personali a titolo di "controprestazione"[63], tenendo, però, presente che al fine di stabilire la legittimità del trattamento dei dati personali – forniti a titolo di "prezzo" – si deve trovare una difficile conciliazione tra quanto la normativa contenuta nella Dir. 2019/770/UE consente di disporre dei propri dati, e quanto il Reg. UE 2016/679 restringe e tutela tale possibilità[64].

57. Ricciuto 2020, p. 660.

58. D'altra parte, la Direttiva 2019/2161/UE, al considerando 31, evidenzia che "I contenuti e i servizi digitali sono spesso forniti online nell'ambito di contratti che non prevedono, da parte del consumatore, il pagamento di un prezzo, bensì la comunicazione di dati al professionista", e, assimilando tale fattispecie alla tradizionale ipotesi dello scambio tramite "moneta", auspica che sia assoggettata alle stesse norme.

59. EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts or the supply of digital content*, cit., nel quale il Garante "mette in guardia contro nuove disposizioni che introducono il concetto che le persone possono pagare con i propri dati, nello stesso modo in cui pagano in denaro".

60. La versione originaria della Proposta di direttiva presentata dalla Commissione conteneva una diversa formulazione dell'art. 3, par. 1, il quale qualificava espressamente la fornitura di dati personali come "controprestazione non pecuniaria" effettuata in cambio della fornitura di servizi o contenuti digitali. Inoltre, nel considerando 13 dava atto che "Nell'economia digitale, gli operatori del mercato tendono spesso e sempre più a considerare le informazioni sulle persone fisiche beni di valore comparabile al denaro. I contenuti digitali sono spesso forniti non a fronte di un corrispettivo in denaro ma di una controprestazione non pecuniaria, vale a dire consentendo l'accesso a dati personali o altri dati".

61. Senigaglia 2020.

62. Il riferimento qui è alla Direttiva 2019/770/UE.

63. D'Ippolito 2022, p. 55.

64. Battelli 2022, p. 5.

È discusso in dottrina se tali modelli negoziali possano effettivamente rappresentare un vantaggio per gli individui[65]. Questo dubbio è occasionato dal fatto che spesso gli utenti non sono a conoscenza né del reale valore dei loro dati né dello scambio che stanno ponendo in essere, soprattutto per quanto attiene alla fornitura "gratuita" di prodotti/servizi digitali.

Il nodo cruciale dello scambio diviene, dunque, il consenso dell'interessato, quale atto giuridicamente complesso, tramite il quale l'interessato esercita il proprio diritto all'autodeterminazione informativa[66]. Esso svolge una funzione conformativa dell'oggetto del contratto di fornitura di servizi e contenuti digitali contro dati personali, il quale consiste nel regolamento del rapporto interessato-titolare del trattamento, all'interno del quale il titolare acquisisce poteri di uso, godimento ed eventualmente ulteriore cessione dei dati dell'interessato. È, infatti, attraverso il consenso che l'interessato può delimitare le finalità, per il cui perseguimento viene concesso l'utilizzo delle informazioni personali.

Una recente novità, elaborata dalle imprese al fine di bilanciare la necessità di raccogliere e trattare i dati degli utenti e il rispetto dei diritti degli stessi, riguarda la tendenza alla remunerazione del consenso al trattamento dei dati personali, assunto come parte di uno scambio tra dati e servizi. Si tratta del fenomeno del c.d. "*cookie-or-pay wall*", o semplicemente "*paywall*", discusso dal Presidente dell'Autorità Garante per la protezione dei dati personali nella Relazione annuale sull'attività del 2022. Il *paywall* consiste in una modalità tramite cui l'utente è messo in condizione di accedere a determinati contenuti web, potendo scegliere tra le alternative del rilascio del consenso ai *cookie* o del pagamento di un prezzo. Si tratta quindi di un vero e proprio modello, definito "*consent or pay model*", che consentirebbe alle imprese di trattare dati, principalmente per finalità di marketing, rimettendo la scelta al singolo utente.

Utilizzato, per la prima volta, da alcune testate giornalistiche, il *cookie wall* è recentemente apparso nei servizi forniti dalla società Meta, all'interno dei quali veniva proposto agli utenti la possibilità di sottoscrivere un abbonamento per l'accesso ai servizi – in particolare Facebook ed Instagram – in alternativa al modello pubblicitario basato, invece, sul trattamento dei dati personali[67].

Il tema del *cookie wall* è stato oggetto di numerose osservazioni da parte delle Autorità garanti europee, le quali hanno assunto posizioni diverse dal 2019, adottando linee guida dal diverso tenore[68], tra cui rientrano anche quelle dettate dal Garante italiano per la protezione dei dati. Quest'ultimo, nelle linee guida aggiornate nel giugno 2021, ha affermato che non è escluso che lo scrolling o il *cookie wall* possano rappresentare delle procedure di acquisizione del consenso lecite, se queste consistono in una delle componenti di un più articolato processo, che consente al soggetto interessato di manifestare in modo inequivoco e consapevole il proprio consenso. In conformità con il principio dell'*accountability*, infatti, il titolare del trattamento può autonomamente individuare soluzioni adeguate e conformi alla disciplina sul trattamento dei dati al fine di ottenere il consenso al trattamento. Con particolare riguardo all'acquisizione del consenso online, tale condizione può tradursi nella possibilità per i titolari del trattamento di adottare delle modalità alternative ed equivalenti, tali da assicurare, in ogni caso, la non equivocabilità del consenso.

65. Mursia–Trovato 2021.

66. Per un approfondimento si v. Spatuzzi 2021, p. 373.

67. In sostanza, la proposta offrirebbe agli utenti la scelta di continuare ad accedere ai servizi "gratuitamente", con pubblicità personalizzate, o di pagare un costo di circa 9,99 euro al mese – che salirebbe a circa 12,99 euro al mese su dispositivi mobili – per versioni dei servizi senza pubblicità. Sul punto v. Agenda Digitale, *Pagare o farsi tracciare dalle big tech: il bivio che cambierà Internet*, 3 ottobre 2023.

68. In particolare, l'Autorità garante dei Paesi Bassi condanna l'approccio definito "*take it or leave it*" insito nel *cookie wall,* denunciandone l'illiceità. Al contrario, l'ICO (l'Autorità garante per la protezione dei dati britannica), sostenendo la necessità di un contemperamento del diritto alla protezione dei dati personali con altri diritti fondamentali, quali la libertà di iniziativa economica, ritiene che non sempre il *cookie wall* può essere considerato "*intrusive*". Infine, sia l'Autorità garante francese (CNIL) sia quella spagnola (AEPD), condividendo quanto affermato dall'Autorità olandese, esprimono un giudizio negativo sui *cookie wall*.

Tanto premesso, è possibile, inoltre, osservare come né la posizione del Garante né tantomeno le discipline contenute nel GDPR e nella Dir. 2019/770/UE porrebbero effettivi divieti o limitazioni all'utilizzo del *cookie wall*, fermo restando l'adozione di un sistema che consente al titolare del trattamento di rispettare quanto previsto sia con riguardo alle caratteristiche del consenso sia per quanto riguarda la corretta ed esaustiva informazione al consumatore.

Analizzando la tecnica di *wall* utilizzata, l'accesso al sito è subordinato alla scelta alternativa dell'utente di sottoscrivere un abbonamento o di prestare il consenso ai mezzi di tracciamento. In questo modo l'utente è immediatamente informato sulle modalità di visualizzazione e fruibilità del sito ed è posto nella posizione di scegliere, selezionando consapevolmente una delle due modalità alternative proposte. Il consenso può, quindi, dirsi: libero, in quanto l'interessato dispone di una scelta effettiva; informato, per la presenza della *cookie policy*, in cui si spiega l'identità del titolare, le finalità del trattamento, nonché le tipologie di dati trattati; specifico, in quanto è espresso per una determinata finalità. La soluzione dei *cookie wall*, dunque, consentirebbe di rispettare le caratteristiche del consenso richieste dalla normativa sulla protezione dei dati[69].

Tuttavia, sul tema è recentemente intervenuto il Comitato europeo per la protezione dei dati (EDPB) che ha escluso la validità di un consenso prestato per usufruire di un servizio fornito da una grande piattaforma digitale, come nel caso di specie Facebook, in alternativa al pagamento di un prezzo, notando che a fronte di una scelta binaria tra il consenso alla profilazione per finalità pubblicitarie e il pagamento di un abbonamento, il consenso non può dirsi realmente libero[70]. Al fine di garantire che l'utente effettui una scelta reale, infatti, il Comitato specifica che "i titolari dovrebbero prendere in considerazione anche l'offerta di un'ulteriore alternativa gratuita"[71]. In assenza di alternative gratuite che consentano all'utente di accedere allo stesso servizio, questo si troverebbe infatti a dover affrontare una conseguenza finanziaria, dovendo pagare un compenso per poter usufruire del servizio. Inoltre, le modalità con cui viene offerto il servizio e il corrispettivo non dovrebbero essere tali da inibire di fatto gli interessati-consumatori a compiere una scelta libera, spingendolo ad acconsentire. Pertanto, la tariffa non dovrebbe essere inappropriatamente alta e tenendo conto dell'essenzialità del servizio.

Pur tenendo a mente queste condizioni, non può farsi a meno di notare come lo stesso impianto del c.d. *paywall* rischia di arrecare un pregiudizio al più generale principio dell'uguaglianza, con una sostanziale contraddizione in termini. I servizi e contenuti online, e più in generale Internet, hanno avuto una rapida ed ampia diffusione, in quanto consentivano a chiunque di navigare in Internet ed accedere ai contenuti gratuitamente. Gli stessi social network offrivano la possibilità di creare un account senza la previsione di un corrispettivo monetario, permettendo la più ampia fruizione del servizio. Tuttavia, con l'installazione di *wall* da parte delle imprese, che obbligano così l'utente ad effettuare la scelta se fornire il consenso al trattamento dei dati o pagare il prezzo richiesto, vengono a differenziarsi gli utenti sulla base della loro condizione economica. Sebbene l'autorità danese abbia tentato di sopperire a tale questione, fissando il limite del "prezzo ragionevole", coloro i quali non dispongano di risorse sufficienti per pagare un compenso, seppur minimo, al fine di accedere ai servizi o contenuti, senza subire il trattamento dei propri dati, si trovano così costretti a "vendere" la propria privacy. In quest'ottica quindi per questa

69. V. Linee Guida dell'Agenzia danese per la protezione dei dati, *Brug af cookie walls*, 20 febbraio 2023, nelle quali sono indicati quattro criteri che formano la base da cui partire per la valutazione delle pratiche tramite cui un'azienda condiziona l'accesso ai suoi contenuti al consenso dei visitatori.

70. EDPB, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, 17 aprile 2024.

71. "Questa alternativa […] può essere una versione del servizio con una diversa forma di pubblicità che comporta il trattamento di meno (o nessun) dato personale, ad es. pubblicità contestuale o generale o basata su argomenti selezionati dall'interessato da un elenco di argomenti di interesse. Ciò è legato anche al principio di minimizzazione dei dati: i titolari del trattamento dovrebbero garantire che vengano trattati solo i dati personali necessari allo scopo di pubblicare tale pubblicità", *ivi*, p.to 74.

fetta di utenti, il consenso prestato al trattamento dei dati perde il requisito della libertà, non essendo prevista una valida alternativa per accedere al servizio. È inconferente anche l'argomento secondo cui gli utenti resterebbero liberi di non usufruire del servizio, in quanto, come nel caso dei servizi offerti dal gruppo Meta, si tratta di strumenti divenuti ormai imprescindibili per la partecipazione alla vita sociale[72].

3. Il caso Facebook tra Italia e Germania

Una volta resosi evidente che nell'economia digitale, in cui l'utente assume al contempo la qualifica di consumatore, a fronte del valore assunto dai dati, si creano problemi di sovrapposizione tra la disciplina in materia di protezione dei dati personali e quella derivante dalla tutela degli interessi dei consumatori e del mercato concorrenziale, si deve dar nota delle conseguenti ricadute in termini di sovrapponibilità delle competenze delle rispettive Autorità[73]. Il tema viene in luce nell'ambito delle "due saghe"[74] giurisdizionali, svoltesi parallelamente in Italia e in Germania, e scaturite dal confronto tra le Autorità garanti della concorrenza e del mercato nazionali, da un lato, e la società Facebook (nel frattempo divenuta Meta), dall'altro.

Come noto, la vicenda italiana si è conclusa con la sentenza 2631 emanata dalla sez. VI del Consiglio di Stato il 29 marzo 2021, mentre il caso tedesco è poi sfociato in una pronuncia di respiro europeo, vale a dire la sentenza del 4 luglio 2023 della Corte di giustizia dell'Unione europea, con la quale si è presentata l'occasione per abbozzare, a livello europeo, le linee di una cooperazione tra l'Autorità garante per la protezione dei dati personali e l'Autorità garante per la concorrenza e il mercato, seguite poi dal Consiglio di Stato che, in una vicenda successiva, ne ha ripreso, come vedremo, i passaggi salienti, cercando di ricomporre un sistema delle autorità indipendenti, incentrato sul dialogo e sulla cooperazione, con la sentenza n. 497 del 2024.

In breve, con la delibera 27438/2018 l'AGCM aveva irrogato a Facebook una sanzione di dieci milioni di euro per pratiche commerciali scorrette poste in essere a danno degli utenti[75]. Facebook, a sua volta, aveva impugnato queste decisioni, portando il caso prima al TAR Lazio e poi al Consiglio

72. BGH 23 giugno 2020 – KVR 69/19, § 58: "l'uso del forum a fini di reciproco scambio ed espressione di opinioni è di particolare importanza a causa dell'elevato numero di utenti e degli effetti di rete".

73. Moretti 2022, p. 98.

74. Di "saga teutonica" parlano Pardolesi–Van den Bergh–Weber 2020, p. 513. Cfr. anche Van den Bergh–Weber 2020, pp. 29-52. Sul tema v. anche Davola 2021; Midiri 2020.

75. Su segnalazione dell'Associazione Altroconsumo, l'AGCM aveva accertato con delibera n. 27432/2018 la natura illegittima di due pratiche, aventi ad oggetto lo scambio e l'utilizzo a fini commerciali dei dati degli utenti, messe in atto da Facebook. In particolare, la pratica a), consisteva in una "pratica ingannevole" posta in essere in violazione degli artt. 20, 21 e 22 del Codice del consumo, in virtù del fatto che il professionista, al momento della registrazione dell'utente alla piattaforma, non fornisse immediate e adeguate informazioni relative all'attività di raccolta e utilizzo dei dati che gli venivano ceduti, celando l'intento commerciale. Al contrario, l'iscrizione avveniva in presenza di un *claim*, contenuto nella pagina di iscrizione, che affermava: "Iscriviti. È gratis e lo sarà per sempre". In tal modo induceva l'utente ad assumere una decisione di natura commerciale che altrimenti non avrebbe preso, a parere dell'Autorità. La pratica b), invece, integrava l'ipotesi di "pratica aggressiva", in violazione degli artt. 20, 24 e 25 del Codice del consumo, in ragione del fatto che Facebook esercitava un indebito condizionamento nei confronti del consumatore, costringendolo a prestare il consenso a FB e a terzi al trattamento dei dati per finalità informative e/o commerciali, in cambio dell'utilizzo del servizio. Il consenso, secondo l'Autorità, veniva prestato in modo inconsapevole e automatico, attraverso un sistema di preselezione dello stesso, idoneo ad indurre a mantenere attivo il trasferimento e l'uso dei propri dati da e verso terzi operatori, per evitare di subire limitazioni nell'utilizzo del servizio, che conseguirebbero alla deselezione, residuando in capo al soggetto interessato la sola facoltà di *opt-out*. L'AGCM aveva, dunque, proceduto ad irrogare una sanzione dall'importo di dieci milioni di euro – cinque per la "pratica a)" e cinque per la "pratica b)" –, vietando contestualmente l'ulteriore diffusione della pratica ingannevole e disponendo la pubblicazione di una dichiarazione rettificativa sulla homepage del sito internet aziendale per l'Italia, sull'app Facebook e sulla pagina personale di ciascun utente italiano registrato.

di Stato, adducendo il difetto assoluto di attribuzione dell'AGCM, sia perché in realtà non si sarebbe trattato di pratiche commerciali, non essendovi stato il pagamento di un corrispettivo patrimoniale da parte degli utenti, sia perché la questione sarebbe stata, in realtà, da inquadrare nella materia "privacy" e sussunta nelle norme del Regolamento UE 2016/679, non in quello dei diritti dei consumatori[76].

La sez. I del TAR Lazio, tuttavia, pronunciandosi con le sentenze nn. 260/2020 e 261/2020, aveva accolto solo parzialmente il ricorso della società, annullando la sanzione relativa alla pratica b) – in virtù del fatto che non sono stati riscontrati i presupposti per qualificare in termini di aggressività la condotta – ma confermando la sanzione relativa alla pratica a), in quanto condivisibile il giudizio di ingannevolezza rinvenuto nel comportamento dell'azienda. Per quanto attiene il dibattito sulla natura dei dati personali e la conseguente competenza rispetto alla loro tutela, il Tribunale regionale era intervenuto affermando che, contrariamente a quanto sostenuta da Facebook, i dati personali costituissero "un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto"[77], ravvisando la necessità di prevedere accanto agli strumenti di tutela tipici del diritto alla protezione dei dati personali, anche delle garanzie del dato quale oggetto di scambi commerciali, riconoscendo gli obblighi di chiarezza, completezza e non ingannevolezza imposti agli operatori dal legislatore dalla disciplina posta a tutela del consumatore ed escludendo, altresì, la sovrapponibilità del piano della tutela della privacy e di quello della protezione del consumatore[78].

Contro la decisione del TAR Lazio entrambe le parti in causa hanno presentato ricorso al Consiglio di Stato, il quale, dopo aver proceduto alla riunione degli appelli, li ha respinti, confermando la sentenza del TAR[79].

Nella sentenza n. 2631/2021, la sez. VI del Consiglio di Stato si è confrontata con il problema della "non commercialità dei dati personali", da cui deriverebbe la non riconducibilità del loro trattamento al diritto consumeristico. Su questo punto Facebook ha incentrato la propria difesa, in quanto, sposando la tesi della natura di diritto fondamentale della protezione dei dati personali, ha sostenuto che la non patrimonialità di tali dati rende di fatto inapplicabile la disciplina in materia consumeristica alla tutela dei dati personali, cui è rivolta, in via esclusiva, la specifica normazione recata dal Regolamento eurounitario n. 679/2016. Di conseguenza, Facebook ha sostenuto che la competenza a giudicare nel caso di specie dovesse essere attribuita all'Autorità capofila[80], ovvero quella irlandese[81].

76. Nella memoria finale depositata in giudizio, la società Meta ha affermato, infatti, che l'Autorità antitrust agirebbe "sulla base di premesse erronee ed al di là delle proprie competenze nella misura in cui utilizza le norme a tutela del consumatore per analizzare le condotte che dovrebbero essere valutate sulla base della normativa sulla privacy e sul trattamento dei dati personali".
77. TAR Lazio, sez. I, 10 gennaio, 2020 n. 261, § 6.
78. *Ivi,* § 10: "il valore economico dei dati dell'utente impone al professionista di comunicare al consumatore che le informazioni ricavabili da tali dati saranno usate per finalità commerciali che vanno al di là della utilizzazione del social network: in assenza di adeguate informazioni, ovvero nel caso di affermazioni fuorvianti, la pratica posta in essere può quindi qualificarsi come ingannevole".
79. Ciò in quanto il Consiglio di Stato ha ritenuto, da una parte, non sussistente alcun elemento di travisamento o manifesta irrazionalità né per quanto attiene ai parametri normativi della scorrettezza delle pratiche commerciali sub a), né con riguardo alla proporzionalità delle sanzioni ingiunte dall'AGCM, e condividendo, dall'altra, le ragioni dei giudici di prime cure relativamente alla "non aggressività" della pratica commerciale sub b) operata da Facebook.
80. L'autorità di controllo capofila è disciplinata dall'art. 56 GDPR e consiste nell'autorità dello stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.
81. Pagnanelli 2022, pp. 17-18, osserva che questa chiara opzione di disciplina presentata da Facebook potrebbe nascondere, in realtà, la percezione, per l'azienda, che la disciplina privacy sia "meno severa" rispetto a quella consumeristica.

Diversamente, il Collegio non è parso aderire all'idea del dato persona come *res extra commercium*, ma, pur evitando di assumere una posizione netta – come quella del TAR Lazio – sulla qualificazione giuridica dei dati personali, ha privilegiato una concezione di patrimonializzazione del dato secondo cui tale fenomeno "costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali". Pertanto, il Consiglio di Stato ha scisso il profilo privacy e quello antitrust, intendendo "i due "diritti" quali distinte categorie settoriali che sono disciplinate da normative speciali e quindi non sovrapponibili tra di loro", sottolineando che la pratica ingannevole risiede nello sfruttamento, inconsapevolmente per l'utente, dei dati offerti al momento dell'iscrizione. Proprio per questo, l'utente, che "si trasforma tecnicamente in 'consumatore' nel momento in cui rende disponibili i propri dati al fine di potere utilizzare gratuitamente i servizi offerti dalle società", resta erroneamente convinto che il conseguimento dei vantaggi collegati con l'accesso alla piattaforma sia gratuito. Così, secondo i giudici di Palazzo Spada, ritenere del tutto a sé stante il settore di tutela dei dati personali determinerebbe l'esclusione dell'applicabilità di ogni altra disciplina giuridica, che si tradurrebbe nella riduzione delle tutele garantite alle persone fisiche. I giudici considerano, invece, la disciplina in materia di pratiche commerciali sleali – Direttiva 2005/29 – e quella presente nel Regolamento 2016/679 tra loro complementari, contribuendo insieme a garantire una "tutela multilivello" che, anzi, incrementa "il livello di garanzia dei diritti delle persone fisiche" anche, e soprattutto, "quando un diritto personalissimo sia sfruttato a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore"[82].

4. La decisione della Corte di giustizia: la necessaria cooperazione delle autorità amministrative indipendenti

Come già osservato, nel frattempo, in Germania, si stava sviluppando una vicenda del tutto parallela[83].

Nel 2019, il Bundeskartellamt aveva sanzionato Facebook per abuso di posizione dominante, contestando la raccolta di dati senza esplicito consenso degli utenti da siti terzi. Ha ritenuto che questa pratica violasse il GDPR e il Bundesdatenschutzgesetz (BDSG), configurando un abuso di posizione dominante poiché gli utenti non avevano scelta se non accettare le condizioni imposte da Facebook[84].

In sede cautelare, l'Oberlandesgericht di Düsseldorf aveva bloccato la decisione, sollevando dubbi sulla mancanza di prova del pregiudizio alla concorrenza e sul nesso di causalità tra l'abuso di posizione dominante e la lesione del diritto degli utenti all'autodeterminazione, adducendoli come vizi della motivazione, sostenendo quindi che l'uso dei dati fosse legittimo, dato il consenso degli utenti, ed escludendo l'abuso di posizione dominante[85].

Tuttavia, il Bundesgerichtshof aveva, a sua volta, ribaltato la decisione del giudice di Düsseldorf, affermando che l'assenza di alternative per gli utenti costituisse un abuso di posizione dominante, indipendentemente dal consenso al trattamento dei dati, in quanto lesivo del diritto all'autodeterminazione informativa. I giudici di Karlsruhe ravvisavano "il maggior *vulnus* nell'elisione della possibilità di scelta"[86], da cui discende un pregiudizio del diritto del consumatore ad autodeterminarsi con conseguente abuso della posizione dominante dell'azienda. Secondo i giudici del Tribunale supremo, infatti, la decisione di Facebook di non mettere a disposizione opzioni tra cui scegliere nel momento in cui un utente decide di usufruire dei servizi di Facebook – decisione che comporta la mancata possibilità per gli utenti di scegliere di utilizzare Facebook senza condividere i propri dati

82. Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631, § 7.

83. Il caso viene trattato in Laviola 2022, p. 28 ss; Midiri 2021, pp. 111 ss.

84. L'Autorità aveva, infatti, ritenuto che i termini di servizio, apposti in violazione delle disposizioni del GDPR, fossero da considerare abusivi ai sensi del §19 (1) GWB. L'acronimo GWB sta per *Gesetz gegen Wettbewerbsbeschränkungen*, ossia la legge tedesca contro le restrizioni della concorrenza, modificata il 18 gennaio 2021. In particolare, la sezione 19, lett. a), del GWB disciplina l'abuso di posizione dominante.

85. OLG Düsseldorf NZKart 2019, 495 – Facebook.

86. Laviola 2022, p. 41.

conformemente alle modalità stabilite – determinava una lesione dell'autonomia decisionale con tanto di violazione del diritto costituzionalmente garantito all'autodeterminazione informativa[87]. Questa mancanza, secondo i giudici, non poteva essere colmata dalla possibilità che l'utente abbia a disposizione di rinunciare completamente all'utilizzo del social network, in quanto, al giorno d'oggi, esso è considerato uno strumento imprescindibile di partecipazione alla vita sociale[88].

Così, pressoché contemporaneamente, nel marzo 2021 – e per di più nel corso della stessa settimana –, le due "saghe" sono giunte a un punto di svolta decisivo.

Come si è visto, la sentenza del Consiglio di Stato del 29 marzo ha, infatti, posto l'ultima parola sul caso scaturito dalla sanzione dell'AGCM a Facebook, successivamente impugnata dinanzi al Tar Lazio. In un'udienza di solo cinque giorni prima, il 24 marzo, l'Oberlandesgericht di Düsseldorf aveva rinviato in via pregiudiziale alla Corte di giustizia dell'Unione europea la soluzione del caso tedesco[89].

Mentre si chiudeva la vicenda italiana, cominciava quella europea.

La principale questione su cui è stata interrogata la Corte di giustizia attiene al fatto se sia compatibile con gli artt. 51 e ss. GDPR che un'autorità diversa da quella preposta al controllo sulla liceità e correttezza dei trattamenti di dati personali – nel caso di specie l'Autorità garante della concorrenza e del mercato –, accerti, nell'ambito dell'esame di abuso di posizione dominante da parte di un'impresa ai sensi del diritto della concorrenza, che le condizioni contrattuali applicate da un operatore siano conformi al GDPR e, in caso di esito negativo, imponga di porre fine a tale violazione.

La Corte ha preliminarmente osservato che, ai sensi dell'art. 5 del Regolamento n. 1/2003, "le autorità nazionali garanti della concorrenza sono competenti ad adottare decisioni che constatino un abuso di posizione dominante da parte di un'impresa, ai sensi dell'art. 102 TFUE, il cui obiettivo consiste nell'istituire un regime atto a garantire che la concorrenza non sia falsata nel mercato interno, tenuto conto anche delle conseguenze di un tale abuso per i consumatori di tale mercato"[90]. Nell'ambito dell'adozione di una decisione di questo tipo è possibile, infatti, che un'autorità garante della concorrenza debba valutare, sulla base di tutte le circostanze del caso di specie, se il comportamento dell'impresa in posizione dominante abbia l'effetto di ostacolare, tramite il ricorso a mezzi diversi da quelli su cui si impernia la concorrenza normale tra prodotti o servizi, la conservazione del grado di concorrenza esistente sul mercato o lo sviluppo di detta concorrenza[91]. A tal fine, dunque, può risultare necessario che l'autorità garante della concorrenza dello Stato membro interessato esamini anche la conformità del comportamento dell'impresa a norme diverse da quelle rientranti nel diritto alla concorrenza, quali – per quel che rileva in questo scritto – le norme in materia di protezione dei dati personali previste dal GDPR.

Tuttavia, quando l'autorità nazionale garante della concorrenza ravvisi una violazione del GDPR, alla luce degli obiettivi perseguiti dalle norme delle diverse discipline, essa non si sostituisce alle autorità di controllo istituite da tale regolamento, ma la valutazione effettuata dall'autorità garante della

87. Come afferma il BGH 23 giugno 2020 § 102: "il diritto all'autodeterminazione informativa garantisce all'individuo la possibilità di esercitare un'influenza differenziata sul contesto e la maniera in cui i propri dati sono resi accessibili ai terzi e usati da loro"; e ha un impatto anche quando "s'interpretano le clausole generali del diritto civile, cui il § 19 Gwb può essere ricondotto".

88. BGH 23 giugno 2020 – KVR 69/19, cit., § 58 cit.

89. "La questione se Facebook stia abusando della sua posizione dominante come fornitore sul mercato tedesco dei social network perché raccoglie e usa i dati dei suoi utenti in violazione del GDPR non può essere decisa senza fare riferimento alla CGUE, essendo essa responsabile dell'interpretazione del diritto europeo" (OLG 24 marzo 2021).

90. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 46.

91. Come rilevato nelle conclusioni dell'Avvocato generale Rantos del 20 settembre 2022, causa C-252/21, *Meta Platforms Inc., già Facebook Inc., Meta Platforms Ireland Limited, già Facebook Ireland Ltd., Facebook Deutschland GmbH contro Bundeskartellamt*, par. 23. In tal senso, v. sentenza del 25 marzo 2021, *Deutsche Telekom/Commissione*, C-152/19 P, EU:C:2021:238, p.ti 41 e 42).

concorrenza in merito alla violazione del GDPR è limitata al solo scopo di constatare un abuso di posizione dominante e di imporre misure volte a far cessare tale abuso secondo le norme di diritto della concorrenza. È chiaro, quindi, che detta autorità non realizza alcuna invasione della sfera di competenza dell'autorità di protezione dei dati dal momento che – come rilevato dalla Corte[92] – non viene esercitato alcuno dei compiti di cui all'art. 57 GDPR, né si fa uso dei poteri riservati all'autorità di controllo in forza dell'art. 58 del medesimo regolamento.

La Corte tuttavia puntualizza che "nel caso in cui un'autorità nazionale garante della concorrenza ritenga necessario pronunciarsi, nell'ambito di una decisione relativa ad un abuso di posizione dominante, sulla conformità o sulla non conformità al GDPR di un trattamento di dati personali effettuato dall'impresa in questione, tale autorità e l'autorità di controllo interessata o, se del caso, l'autorità di controllo capofila competente ai sensi di tale regolamento devono cooperare tra loro al fine di garantire un'applicazione coerente di tale regolamento"[93]. Viene così richiamato il principio di leale cooperazione tra le autorità nazionali[94], al fine di garantire un'applicazione coerente del GDPR. Tale principio obbliga l'autorità garante della concorrenza, nel caso in cui ritenga necessario controllare il rispetto da parte di un'impresa delle disposizioni del regolamento, a concertarsi con l'autorità nazionale di controllo competente e, quindi, a verificare se tale comportamento – o un comportamento simile – sia già stato oggetto di una decisione da parte di tale autorità o, ancora, della Corte. Nell'ipotesi in cui l'autorità garante privacy competente si fosse già pronunciata, l'autorità garante della concorrenza non potrebbe discostarsi da tale pronuncia, restando, però, libera di trarre conclusioni utili per l'applicazione del diritto della concorrenza.

In forza, dunque, del principio di leale collaborazione, la Corte specifica che laddove un'autorità garante della concorrenza nutra dubbi sulla portata della decisione dell'autorità garante della privacy, laddove il comportamento di un'impresa sia, al contempo, oggetto di esame da parte di tali autorità privacy, nazionali o capofila, o laddove in assenza di un'indagine di dette autorità, l'autorità nazionale garante della concorrenza ritenga che un comportamento di un'impresa non sia conforme alle disposizioni del GDPR, quest'ultima "deve consultare l'autorità nazionale di controllo del regolamento e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione"[95].

In definitiva, dunque, la CGUE afferma la competenza di un'autorità garante della concorrenza di uno Stato membro a constatare che "le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare

92. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 48.

93. *Ivi*, p.to 52.

94. Cfr. art 4, par. 3, TUE il quale sancisce che "In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati". Secondo una giurisprudenza costante, infatti, l'obbligo degli Stati membri di assistersi reciprocamente, nell'adempimento dei compiti derivanti dai Trattati, di adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, nonché di astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione, include anche le loro autorità amministrative (v., in tal senso, sentenze del 7 novembre 2013, *UPC Nederland*, C518/11, EU:C:2013:709, p.to 59, nonché del 1° agosto 2022, *Sea Watch*, C-14/21 e C-15/21, EU:C:2022:604, p.to 156).

95. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 63. Nel caso di specie, risulta che, prima di giungere all'adozione della propria decisione, l'autorità federale garante della concorrenza abbia posto in essere una cooperazione con le autorità garanti della protezione dei dati tedesche (in particolare, il *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), commissario federale per la protezione dei dati e la libertà d'informazione, Germania, lo *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, il commissario per la protezione dei dati e la libertà d'informazione di Amburgo, competente riguardo a Facebook Deutschland, nonché la *Data Protection Commission* (DPC), ossia l'autorità per la protezione dei dati, Irlanda), senza ricevere obiezioni da parte di questi in merito al proprio intervento (cfr. p.ti 555 e 556 della sua decisione del 6 febbraio 2019).

l'esistenza di un tale abuso"[96], fermo restando però il rispetto dell'obbligo di leale cooperazione con le autorità di controllo.

Da un'analisi della sentenza, occorre tuttavia notare che se, da una parte, è stata ribadita la centralità del consenso dell'interessato, nel caso di trattamenti effettuati dal titolare di un social network online, dall'altra, la dirimente questione di fondo rimessa alla Corte, in merito alla possibilità che i dati personali abbiano o meno valore economico – su cui risulta essenziale un parere della Corte – è rimasta sostanzialmente senza risposta, non avendo i giudici preso una posizione netta in merito. La Corte, infatti, ha affermato la competenza dell'Autorità antitrust a sindacare il rispetto alle disposizioni del GDPR da parte di un operatore di un social network, riconoscendo che "i dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese dell'economia digitale" e che, pertanto, "escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione"[97]. Tuttavia, non ha ammesso una generale competenza dell'autorità garante della concorrenza, confermando così l'economicità dei dati, ma si è limitata a constatarne la competenza nella sola ipotesi di indagine di abuso di posizione dominante, vincolandola, inoltre, ad una cooperazione fattiva con le autorità garanti della protezione dei dati personali, di cui devono tenersi in considerazione qualsiasi decisione o indagine.

Pertanto, tale pronuncia, sebbene rappresenti un ulteriore passo in avanti nell'ottica di una stretta sinergia tra le attività svolte dalle diverse autorità amministrative indipendenti e di coordinamento tra le diverse normative al fine di costruire un *enforcement* armonizzato di regole volte alla costruzione del *Digital Single Market*, lascia sospesa la questione se i dati personali possano o meno essere considerati un bene economico, rimettendo la decisione ai singoli operatori nazionali.

5. Il Consiglio di Stato riafferma il principio leale collaborazione

Le conseguenze della posizione assunta dalla Corte di giustizia con la sentenza 4 luglio 2023 non hanno tardato a presentarsi. Il 15 gennaio 2024, a pochi mesi quindi dalla pubblicazione della sentenza della CGUE, il Consiglio di Stato ha emesso una nuova sentenza sulla questione[98], all'esito del procedimento del c.d. caso Telepass.

In breve, l'AGCM aveva irrogato alla società Telepass S.p.a. e Telepass Broker S.r.l. (d'ora in poi Telepass e Tb) una sanzione pecuniaria di due milioni di euro per pratiche commerciali scorrette in quanto nel comparto dell'*insuretech* fornivano informazioni ingannevoli e/o carenti sulla raccolta e trattamento dei dati degli utenti che richiedevano un preventivo assicurativo relativo a polizze RC auto tramite App Telepass e sulle modalità di preventivazione[99]. Infatti, le società Telepass e Tb e le Compagnie assicurative partner condividevano un *data base* dedicato per la gestione e l'acquisizione di dati assicurativi, separato rispetto alla piattaforma attraverso la quale la stessa Telepass gestiva i dati degli utenti titolari dei dispositivi per i servizi di pagamento in mobilità. Pertanto, nel corso dell'intera procedura digitale, il consumatore non era edotto circa la raccolta e l'utilizzo a fini commerciali dei suoi dati, che Telepass otteneva dalle

96. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 62.

97. *Ivi*, p.to 51.

98. Consiglio di stato, sez. VI, 15 gennaio 2024, n. 497.

99. Su segnalazione dell'Associazione Nazionale Agenti Professionisti di Assicurazione (ANAPA), l'AGCM aveva accertato con delibera n. 28601/2021 l'illegittimità di due condotte poste in essere dalle due società del Gruppo Telepass, in violazione degli artt. 21 e 22, commi 1 e 2 del Codice del Consumo. In particolare, la condotta a), concerneva l'assenza di informativa ai clienti, che richiedevano il preventivo per la polizza RC auto tramite APP Telepass, circa la gestione, conservazione e trasferimento di dati dei clienti dalle compagnie assicurative alla stessa Telepass, la quale li sfruttava a fini commerciali. La condotta b) riguardava l'assenza di indicazione circa i criteri e parametri di riferimento e di selezione del preventivo RC auto proposto, enfatizzando piuttosto la particolare facilità e convenienza della proposta effettuata attraverso l'App.

compagnie assicurative in fase di preventivo, né tantomeno era a conoscenza dei criteri sulla cui base Telepass e Tb proponevano il preventivo RC auto definito "migliore", inducendo in tal modo i consumatori ad assumere decisioni di natura commerciale che altrimenti non avrebbero assunto, a parere dell'autorità.

Avverso tale provvedimento, le società Telepass e Tb hanno inizialmente proposto ricorso dinanzi al TAR Lazio, al fine di ottenere l'annullamento del suddetto provvedimento sanzionatorio, deducendo quale principale motivo di ricorso la violazione, da parte dell'AGCM, delle competenze e delle prerogative del Garante per la protezione dei dati personali, nonché la violazione dei principi di buon andamento dell'azione amministrativa e di leale collaborazione, in quanto era mancato, nel corso del procedimento conclusosi con il provvedimento sanzionatorio dell'AGCM, l'acquisizione del parere del Garante privacy, essendo indubbio che lo stesso fosse necessario nell'ambito dell'esame di un comportamento anticonsumeristico derivante da una condotta violativa delle norme poste a protezione del trattamento dei dati.

Con la sentenza n. 603/2023 il TAR Lazio ha respinto il ricorso[100], inducendo così le società a rivolgersi al Consiglio di Stato per chiedere la riforma della sentenza di primo grado e il conseguente annullamento del provvedimento adottato dall'Antitrust.

In giudizio si sono costituiti anche l'Autorità per le garanzie nelle comunicazioni, il cui parere era stato acquisito dall'Antitrust durante l'istruttoria ai sensi dell'art. 27, comma 6, del Codice del consumo, e il Garante privacy, quest'ultimo a difesa delle proprie prerogative[101].

Sotto il profilo della contaminazione normativa tra il settore consumeristico e quello della tutela dei dati personali ed in ragione dell'ingente rilevanza strategica che i dati hanno assunto nell'ambito dell'attività delle imprese, il Consiglio di Stato ha, in via preliminare, chiarito che "lo spettro amplissimo di ipotesi riconducibili all'attività di trattamento e dunque rilevanti in materia di dati personali delle persone fisiche e quindi ricadenti nella sfera di applicazione del GDPR, esclude, già da solo, che la sostenuta esistenza di compartimenti 'stagni', non permeabili tra loro, tra l'ambito di competenza e dei poteri di AGCM rispetto a quelli di altre Autorità, in particolare del Garante privacy, possa militare nel senso di escludere 'a priori' qualsiasi forma di collaborazione tra le due Autorità nel corso di una indagine che, seppure fondamentalmente indirizzata circa la compatibilità o meno con la disciplina consumeristica di condotte sviluppate da professionisti, abbia indubbiamente addentellati forti e robuste caratterizzazioni osmotiche con la tutela dei dati personali", potendosi sostenere "una funzionalizzazione tra i comportamenti contestati e la violazione, contemporanea, di discipline normative differenti perché riferite a settori specialistici e quindi la doverosità della cooperazione tra Autorità".

Al fine di giungere alla soluzione del nodo contenzioso principale, palesandosi un conflitto di competenze tra le due diverse Autorità

100. Il TAR infatti ha evidenziato che "il collegamento con l'informativa sulla privacy è solo incidentale e non è dirimente al fine di giudicare della legittimità dei comportamenti contestati. Nel caso di specie rileva l'omissione di informazioni essenziali per consentire ai consumatori il libero e consapevole esercizio delle proprie scelte negoziali, in quanto il piano attinente alla tutela della privacy e, di risulta, la corrispondente competenza del Garante per la protezione dei dati personali costituiscono aspetti del tutto autonomi". Secondo il tribunale, dunque, "non sussisteva alcun obbligo di interpellare il Garante, in quanto non si trattava di richiedere un parere obbligatorio nell'ambito di un settore regolato, ai sensi dell'art. 27, comma 1 bis del Codice del Consumo".

101. Cfr. Atto di costituzione del Garante Privacy, richiamato in sentenza, in cui l'Autorità ha, dapprima, ricordato che vi possono essere fattispecie alle quali si applicano più norme e beni giuridici la cui vigilanza è affidata a soggetti diversi, affermando però che è il principio – avente valore costituzionale – di leale collaborazione fra amministrazioni "ad imporre erga omnes la esigenza di risposte coordinate, soprattutto nei casi, non infrequenti, in cui la condotta possa attivare più apparati sanzionatori e dunque plurimi procedimenti di irrogazione". In riferimento al caso di specie, l'Autorità garante per la protezione dei dati personali ha rilevato come l'AGCM, sebbene abbia acquisito il parere dell'AgCOM e dell'IVASS, ha però omesso di richiedere il parere del Garante privacy, in una fattispecie che, rientrando nella previsione di cui all'art. 130 Codice privacy e attenendo alla libera circolazione dei dati, ricadeva sia in astratto che in concreto sotto la vigilanza del Garante.

indipendenti, i giudici di Palazzo Spada hanno ritenuto necessario fare richiamo alla recente sentenza della Corte di giustizia Ue 4 luglio 2023, superando le evidenti difformità[102] tra le fattispecie poste alla base delle due pronunce, in quanto in entrambe le ipotesi si riscontrano profili di "contiguità e prossimità tra l'indagine dell'Autorità Antitrust e il settore della tutela dei dati personali di competenza dell'autorità di controllo istituita nel paese di riferimento (nel caso il Garante privacy)"[103]. Nella sentenza 4 luglio 2023 era stato chiarito che, quando le autorità nazionali garanti della concorrenza si trovino, nell'esercizio delle loro competenze, ad esaminare la conformità di un comportamento di un'impresa alle disposizioni del GDPR, esse devono concertarsi e cooperare lealmente con le autorità di controllo competenti. Ne consegue che, qualora un'autorità nazionale garante della concorrenza ritenga che un comportamento di un'impresa non rispetti le disposizioni dettate in materia di protezione dei dati personali, l'autorità stessa deve consultare l'autorità di controllo competente in materia di privacy e chiederne la cooperazione, al fine di fugare i propri dubbi o valutare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione. Trovando i principi espressi dalla CGUE piena applicazione al caso in esame, a parere del Consiglio di Stato, si è reso evidente che il mancato coinvolgimento, nel corso dell'istruttoria svolta dall'AGCM, del Garante privacy si sia sostanziato in un vizio procedimentale che ha determinato nel provvedimento finale una patologia rilevante, tale da indurre il Consiglio di Stato ad accogliere il ricorso e ad annullare l'atto sanzionatorio emesso dalla stessa AGCM.

Occorre, a questo punto, evidenziare che la soluzione accolta nella sentenza analizzata in questo paragrafo è stata frutto dell'interpretazione estensiva che i giudici di Palazzo Spada hanno adottato dei principi riscontrati dalla sentenza 4 luglio 2023 CGUE. Come è stato osservato nel precedente paragrafo, quest'ultima non ha riconosciuto una generale e diffusa competenza dell'Antitrust a sindacare il rispetto delle regole in materia di dati personali nello svolgimento delle proprie indagini, ma essa è stata confermata solo nell'ipotesi di esame di abuso di posizione dominante da parte dell'Autorità, fermo restando l'obbligo di cooperazione con il Garante privacy. La sentenza in esame, invece, inserendosi nel solco tracciato dalla precedente sentenza del Consiglio di Stato (sent. n. 2631/2021), circa la commistione tra le due discipline, consumeristica e privacy, ha quindi rappresentato una importante svolta nel delineare i profili della collaborazione richiesta alle due Autorità, estendendo i contorni timidamente delineati dalla Corte di giustizia del principio di leale collaborazione.

6. Conclusioni

In conclusione, l'evoluzione tecnologica ed informatica ha determinato la sistematizzazione dell'attività imprenditoriale e la messa a disposizione di strumenti di circolazione di dati di ogni natura, rendendo la condivisione e l'utilizzo delle informazioni lo strumento necessario all'esercizio dell'attività economica e, più in generale, alla realizzazione di un mercato unico dei dati.

In questo contesto le sfide poste dal progresso tecnologico stanno esponendo il fondamentale diritto alla protezione dei dati personali e l'equilibrio del mercato a rischi nuovi, determinando di conseguenza il legislatore a sviluppare un sistema

102. Il caso concreto posto all'attenzione della Corte di giustizia riguardava, infatti, l'ipotesi di abuso di posizione dominante contestata dall'Autorità antitrust tedesca, la quale, nell'ambito del suo esame, aveva rilevato come la condotta posta in essere dalla società Meta Platforms Ireland violasse le disposizioni in materia di dati personali. È chiara, quindi, la difformità della vicenda tedesca rispetto alla vicenda odierna in cui l'indagine dell'Antitrust si è focalizzata su una condotta anticonsumeristica imputata all'impresa, sebbene entrambe le ipotesi riguardino la sovrapposizione tra la normativa a tutela dei dati personali e la disciplina consumeristica. È interessante anche notare che lo stesso Consiglio di Stato afferma che la vicenda sottopostagli, non attiene alla possibilità o meno, da parte delle società, di patrimonializzare i dati personali dei loro clienti, il che rende il c.d. caso Telepass ulteriormente diverso dal c.d. caso Facebook.

103. "Le deduzioni sviluppate e i principi espressi nella sentenza della Corte di giustizia UE 4 luglio 2023 si attagliano plasticamente al caso in esame e completano le osservazioni illustrate più sopra dal Collegio" (Consiglio di Stato, sez. VI, 15 gennaio 2024, n. 497, p.to 12).

in grado di reinterpretare e riequilibrare il quadro dei poteri e delle libertà che vengono in rilievo.

Tuttavia, la possibilità di governare i dati nel nuovo ecosistema digitale è resa difficile dalla mancanza di un quadro organico di riferimento. I casi analizzati nei precedenti paragrafi hanno infatti fatto luce sul problema di coordinamento tra le diverse normative, in particolare la tutela dei dati personali e la tutela della concorrenza, nonché sulla difficile commistione delle competenze delle rispettive Autorità di controllo. Tale quadro, già di per sé complesso, rischia di complicarsi ulteriormente alla luce dei numerosi provvedimenti adottati a livello europeo. DGA, DA letti di concerto con DMA, DSA, AI Act, NIS 2 e vari altri recenti interventi normativi, sebbene definiscano le regole per disciplinare e controllare il mercato digitale e imbrigliare il potere delle *big tech*, tenendo in considerazione la correlazione, ormai instauratasi tra concorrenza e privacy[104] e prevedendo, al fine di garantire l'equilibrio nel mercato, maggiore trasparenza nei rapporti tra i fornitori e utenti e il controllo da parte di autorità amministrative indipendenti, nascondono il rischio di un'insostenibile frammentazione in termini di sovrapposizioni istituzionali e conflitti tra le diverse autorità designate dagli Stati membri.

Un duplice esempio in tal senso è rappresentato dal Digital Governance Act (DGA) e dal Data Act (DA), i quali hanno come principale obiettivo quello di favorire la condivisione dei dati, nel rispetto del diritto europeo o nazionale in materia di protezione dei dati. Il DGA, che introduce un nuovo quadro normativo per regolare l'intermediazione dei dati e promuoverne pratiche di altruismo in tutta l'Unione europea, all'articolo 13, richiede agli Stati membri di designare una o più autorità competenti per gestire la procedura di notifica relativa ai servizi di intermediazione dei dati. Lo stesso schema viene riproposto nel Data Act che, ai sensi dell'art. 37, attribuisce agli Stati membri la facoltà di istituire nuove autorità o affidare i compiti a quelle esistenti. La flessibilità concessa agli Stati, sebbene presenti profili di ragionevolezza, nella realtà potrebbe creare una sovrapposizione di competenze, in quanto le autorità preesistenti, come chiarisce il DGA stesso all'art. 13, par. 3, mantengono i loro poteri, e il regolamento richiede che si instauri una forte cooperazione tra loro.

Fermo restando che, in un settore delicato come la gestione dei dati e la regolazione delle nuove tecnologie, in cui le interpretazioni normative possono divergere sensibilmente, la cooperazione tra enti con competenze diverse può risultare spesso problematica, occorre notare, tra tutti questi provvedimenti, l'assenza di una legge che definisca un quadro generale in materia di autorità amministrative indipendenti sia in Italia che in Europa. Sarebbe auspicabile, infatti, adottare una legge generale che razionalizzi in modo chiaro i processi e l'organizzazione delle funzioni delle varie autorità indipendenti, o che comunque raccordi le discipline che vengono in rilievo, introducendo eventuali criteri di prevalenza. In altre parole, sarebbero necessarie regole generali riguardanti l'organizzazione degli uffici, le competenze delle singole Autorità e il procedimento istruttorio, includendo anche procedure di coordinamento delle diverse discipline sulle questioni di interesse comune.

La proliferazione normativa e la mancanza di un reale raccordo tra i nuovi provvedimenti e la disciplina in materia di protezione dei dati personali[105] rischiano di tradire l'intento del legislatore europeo di incrementare la fiducia dei consumatori e valorizzare la competitività delle piccole e medie imprese europee. I primi, infatti, avranno difficoltà nell'identificare la normativa di riferimento e l'autorità a cui rivolgersi in caso di violazione dei loro diritti; le seconde invece si troveranno gravate da numerosi obblighi, incisivi quindi della loro libertà di iniziativa economica, il cui mancato rispetto potrà attivare i poteri sanzionatori e ispettivi di una pluralità di soggetti.

Dinnanzi a questo vuoto normativo e a fronte dell'importanza della pluralità di interessi coinvolti,

104. Si tenga presente l'osservazione di Pitruzzella 2019, secondo cui, nel contesto eurounitario, la tutela dei diritti e il buon funzionamento del mercato sono del tutto complementari.

105. Si nota, infatti, che il considerando 4 del DGA specifica che "In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o del diritto nazionale adottato conformemente a tale diritto dell'Unione, il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali dovrebbe prevalere", utilizzando quindi una forma condizionale senza specificare come realmente tale "prevalenza" si manifesta in concreto.

tra i quali la tutela della privacy, la tutela del consumatore e della concorrenza, fondamentale risulta l'intervento della giurisprudenza, prima europea e poi nazionale, nelle cui pronunce è stata di fatto dettata una regola risolutiva del caso concreto, prevedendo un obbligo di leale cooperazione tra le Autorità, sanzionabile con l'annullamento dei provvedimenti adottati.

In un quadro così problematico – in cui al valore personalistico dei dati attinente alla dignità e all'identità della persona viene ad aggiungersi anche un'ulteriore tipologia di valore, il valore economico, ossia il fatto che i dati possano considerarsi dei beni e circolare liberamente nel mercato, ed entrambi vanno tenuti in egual considerazione affinché le esigenze del mercato o della collettività non rischino di determinare un'ingiustificata compressione della libertà del singolo[106] – la giurisprudenza impone dunque una regolazione di tipo partecipativo[107], che coinvolga, oltre al controllo del Garante per la protezione dei dati personali, anche la vigilanza e l'intervento delle altre autorità indipendenti.

Sulla scia della giurisprudenza, specie quella europea, e alla luce delle criticità evidenziate, il 16 gennaio 2025, l'EDPB ha pertanto pubblicato una dichiarazione sull'interazione tra il diritto della concorrenza e la protezione dei dati[108], nella quale, dopo una parte introduttiva in cui spiega lo sviluppo dell'interazione tra le due discipline – chiarendo che, pur trattandosi di "*fields of law that pursue diffent objectives*", hanno dei potenziali punti in comune – suggerisce raccomandazioni volte a migliorare la cooperazione tra le diverse autorità di regolamentazione. All'interno del documento, infatti, l'EDPB ipotizza, fra tutti, la possibilità di una stipulazione tra le autorità di accordi di cooperazione – ad esempio accordi amministrativi, dichiarazioni comuni o protocolli d'intesa – nei quali stabilire i principi e le regole per la cooperazione, nonché una miglior comprensione del rapporto tra le discipline, e nell'ambito dei quali prevedere la formazione all'interno delle singole autorità, di gruppi di lavoro dedicati alla cooperazione e prodromici quindi a costituire un punto di contatto unico per gestire il coordinamento con le altre autorità di regolamentazione.

Tale documento costituisce infine un ulteriore tassello e ulteriore presupposto fondativo del sistema di regolazione dell'ecosistema digitale che, a fronte del repentino evolversi dell'economia digitale, il legislatore europeo sta tentando di delineare, tenendo a mente l'importanza che assume la promozione di sinergie tra le diverse autorità di controllo in modo tale da offrire un'efficace tutela ai diritti fondamentali che vengono in rilievo e creare quel "clima di fiducia" che consentirebbe di "mantenere l'Ue all'avanguardia dell'economia agile basata sui dati, rispettando e promuovendo nel contempo i valori fondamentali che costituiscono i capisaldi delle società europee"[109].

Riferimenti bibliografici

C. Basunti (2020), *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in "Contratto e impresa", 2020, n. 2

E. Battelli (2022), *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono "gratuiti"*, in "I Contratti", 2022, n. 3

106. Laviola 2021, pp. 195-211.

107. EDPS, *Opinion 8/2016, on coherent enforcement of fundamental rights in the age of big data*, 23 settembre 2016, p. 10: "The synergies between the fields of law, which have been discussed intensively in the recent years, could propel closer cooperation between authorities, especially where there is neither guidance nor case law. It is not a question of 'instrumentalising' another area of law but rather of synchronising EU policies and enforcement activities, adding value where a supervisory authority lacks expertise or legal competence in analysing". L'esigenza di un coordinamento tra le due autorità è stata evidenziata anche in altre occasioni, v. *Antitrust, Privacy and Big Data*, discorso dell'EPDS, 3 febbraio 2015, Joint EDPS-ERA Workshop; *Competition Rebooted: enforcement and personal data in Digital Markets*, 24 settembre 2015, Brussels.

108. EDPB, *Position paper on Interplay between data protection and competition law*, 16 gennaio 2025.

109. Commissione europea, *Una strategia per i dati*, COM(2020) 66, 19 febbraio 2020, p. 2.

F. Caggia (2019), *Libertà ed espressione del consenso*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

F. Calisai (2019), *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

E. Cheli (2021), *Conclusioni*, in "Osservatorio sulle fonti", 2021, n. 2

C. Colapietro (2021), *Circolazione dati, automatizzazione, regolazione*, in "Osservatorio sulle fonti", 2021, n. 2

E. Cremona (2021), *Le nuove tecnologie oltre la "grande dicotomia" tra pubblico e privato*, in "La rivista Gruppo di Pisa", 2021, Quaderno n. 3

E. Cremona, F. Laviola, V. Pagnanelli (a cura di) (2022), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, 2022

G. d'Ippolito (2022), *Monetizzazione, patrimonializzazione e trattamento di dati personali*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

A. Davola (2021), *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in "Diritto di internet", 2021, n. 1

A. De Cupis (1982), *I diritti della personalità*, in "Trattato di diritto civile e commerciale", vol. IV, Giuffrè, 1982

A. De Franceschi (2019), *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

S. Elvy (2017), *Paying for privacy and the personal data economy*, in "Columbia Law Review", vol. 117, 2017, n. 6

A. Gentili (2022), *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in "Rivista trimestrale di diritto e procedura civile", 2022, n. 3

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei "data spaces": Data Governance Act e Data Act*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

K. Klonick (2018), *The new governors: the peoples, rules and processes governing online speech*, in "Harvard Law Review", vol. 131, 2018, n. 6

F. Laviola (2022), *Il diritto all'autodeterminazione informativa tra concorrenza e* data protection, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

F. Laviola (2021), *Diritti fondamentali ed efficienza economica nel mercato digitale: tra protezione dei dati personali e tutela della concorrenza*, in "La rivista Gruppo di Pisa", 2021, Quaderno n. 3

G. Malgieri, B. Custers (2018), *Pricing privacy – the right to know the value of your personal data*, in "Computer Law & Security Review", vol. 34, 2018, n. 2

T.W. Malone, J. Yates, R.I. Benjamin (1987), *Electronic markets and electronic hierarchies*, in "Communications of the ACM", vol. 30, 1987, n. 6

V. Mayer-Schönberger, T. Ramge (2018), *Reinventare il capitalismo nell'era dei Big Data*, Egea, 2018

F. Mezzanotte (2018), *I poteri privati nell'odierno "diritto dello sviluppo economico"*, in "Politica del diritto", 2018, n. 3

F. Midiri (2016), *La giuridificazione della protezione dei dati personali*, in L. Ferrara, D. Sorace, B. Marchetti, M. Renna (a cura di), "A 150 anni dall'unificazione amministrativa italiana. La giuridificazione", vol. iii, Firenze University Press, 2016

M. Midiri (2021), *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in "Il diritto dell'informazione e dell'informatica", 2021, n. 2

M. Midiri (2020), *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in "federalismi.it", 2020, n. 14

G. Mirabelli (1993), *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in "Il diritto dell'informazione e dell'informatica", 1993, n. 2

A. Moretti (2022), *Il valore dei dati nell'*European Data Strategy*: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

M. Mursia, C.A. Trovato (2021), *The commodification of our digital identity: limits on monetizing personal data in the European context*, in "MediaLaws", 2021, n. 2

M. Naldi (2018), *Prospettive economiche dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

A. Nicita (2019), *Il dato profilato nella prospettiva economica tra* privacy, propertization, secrecy, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

V. Pagnanelli (2022), *Una "valutazione d'impatto" della privacy sulle Big Tech*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

R. Pardolesi, R. Van den Bergh, F. Weber (2020), *Facebook e i peccati da "Konditionenmissbrauch"*, in "Mercato concorrenza regole", 2020, n. 3

G. Pitruzzella (2019), *L'Europa del mercato e l'Europa dei diritti*, in "federalismi.it", 2019, n. 6

O. Pollicino (2019), *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19

O. Pollicino (2019-a), *New Technology, Algorithms and the Rising of Private (Digital) Powers and new Challenges for Constitutional Law*, in "Eurac research", 11 July 2019

A. Predieri (1997), *L'erompere delle autorità amministrative indipendenti*, Passigli Editori, 1997

G. Resta (2019), *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra direttiva (UE) 2019/770 e il Regolamento UE 2016/679*, in "Annuario del Contratto 2018", 2019

G. Resta (a cura di) (2010), *Diritti esclusivi e nuovi beni immateriali,* UTET, 2010

G. Resta, V. Zeno-Zencovich (2018), *Volontà e consenso nella fruizione dei servizi in rete*, in "Rivista trimestrale di diritto e procedura civile", 2018, n. 2

V. Ricciuto (2020), *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in "Rivista di diritto civile", 2020, n. 3

V. Ricciuto (2018), *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in "Il diritto dell'informazione e dell'informatica", 2018, n. 4-5

V. Ricciuto, C. Solinas (2021), *Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in "Giustiziacivile.com", 2021, n. 5

C. Sartoretti (2019), *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in "federalismi.it", 2019, n. 13

R. Senigaglia (2020), *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in "Contratto e impresa", 2020, n. 2

S. Sica (2001), *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in "Rivista di diritto civile", 2001, n. 6

S. Simitis (1997), *Il contesto giuridico e politico della tutela della privacy*, in "Rivista critica di diritto privato", 1997, n. 4

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal–Rivista di BioDiritto", 2019, n. 1

A. Simoncini, E. Cremona (2021), *European Private Law Integration through Technology: the Constitutional Dimension*, in "Persona e mercato", 2021, n. 2

C. Solinas (2021), *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in "Giurisprudenza italiana", 2021, n. 2

A. Spatuzzi (2021), *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali*, in "Notariato", 2021, n. 4

A. Stazi, F. Corrado (2019), *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 2

K.J. Strandburg (2013), *Free Fall: The Online Market's Consumer Preference Disconnect*, University of Chicago Legal Forum, 2013

R. Van den Bergh, F. Weber (2020), *The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law?*, in "World Competition", vol. 44, 2020, n. 1

V. Zeno-Zencovich (2019), *Do "Data Markets" Exist?*, in "MediaLaws", 2019, n. 2

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0226 • articolo sottoposto a peer review • pubblicato in anteprima il 25 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

ERCOLE DE LUCA – LUISA LODEVOLE

Il nuovo design europeo del mercato dell'energia elettrica e i contratti flessibili: il caso del progetto pilota di Areti "Romeflex"

Il contributo ha ad oggetto la *Electricity Market Reform* tracciata dal Regolamento (UE) 2024/1747 e dalla Direttiva (UE) 2024/1711. Lo studio è stato condotto nell'ambito del progetto di ricerca dal titolo "Tecnologie green" sotto la duplice prospettiva del giurista e dell'ingegnere. Da un lato il dato tecnico-normativo è ricondotto nella cornice più ampia del concetto di energia come bene pubblico e/o utilità privata. Dall'altro lato gli operatori del mercato dell'energia elettrica, principalmente TSOs e DSOs, sono chiamati ad impegnarsi per calare gli obiettivi stabiliti dal *Clean Energy Package*, di decarbonizzazione e neutralità climatica, nei concreti meccanismi di distribuzione e somministrazione dell'energia elettrica. A questo proposito si sottolinea il carattere pionieristico del progetto aziendale di Areti "Romeflex". Esso propone un modello originale di erogazione e consumo dell'elettricità, flessibile ed efficiente, al quale gli utenti possono aderire su base volontaria, remunerata sulla base del principio demand/response. L'adeguamento delle infrastrutture tecnologiche mediante smart grids a criteri di efficienza economica e sostenibilità ambientale comporta la configurazione, grazie alla tecnologia degli smart contract, di nuovi legal framework i c.d. contratti flessibili. Questi processi richiedono assunzione di consapevolezza e responsabilità di tutti i membri della società.

Beni pubblici – Energie rinnovabili – Flessibilità – Smart contract – Sostenibilità ambientale

The new European electricity market design and flexible contracts: the case of Areti's pilot project "Romeflex"

The paper deals with the Electricity Market Reform outlined by Regulation (EU) 2024/1747 and Directive (EU) 2024/1711. The study was carried out as part of the research project entitled *Green Technologies* from the dual perspective of the jurist and the engineer. On the one hand, the technical-normative data is brought back into the broader framework of the notion of energy as a public good and/or private utility. On the other hand, electricity market operators, mainly *TSOs* and *DSOs*, are called upon to embed the goals of decarbonization and climate neutrality set by the *Clean Energy Package*, in the concrete electricity distribution and delivery mechanisms. In this regard, the pioneering nature of *Areti*'s corporate project *Romeflex* is pointed out. It proposes an original model of electricity supply and consumption, flexible and efficient, which users can join on a voluntary and remunerated basis, on the demand/response principle. The adjustment of technological infrastructure through smart grids to criteria of economic efficiency and environmental sustainability involves the configuration of new legal frameworks, with the help of smart contracts technology, the so-called flexible contracts. These processes require the awareness and responsibility of all the members of society.

Public goods – Renewable energy – Flexibility – Smart contract – Environmental sustainability

L. Lodevole è ricercatrice presso il Dipartimento di Giurisprudenza, Università degli Studi di Roma Tor Vergata. E. De Luca è ingegnere, responsabile del Presidio Regolatorio e dei Progetti Finanziati di Areti S.p.a. Il presente studio è stato elaborato grazie alla collaborazione scientifica con Areti S.p.a. e in particolare con il contributo dell'ing. De Luca. Sebbene l'elaborato sia frutto del comune lavoro di progettazione, ricerca e sviluppo, i paragrafi 1 e 10 sono riferibili ad entrambi, E. De Luca è autore dei paragrafi 4 e 5 e L. Lodevole è autrice dei paragrafi 2, 3, 6, 7, 8 e 9.

Sommario: 1. Il nuovo *Electricity Market Design* tracciato dall'Ue: tra diritto pubblico e diritto privato. – 2. L'energia elettrica: da utilità privata a bene pubblico. – 3. Profili giuspubblicistici: il ruolo delle Autorità di regolazione del mercato nel contesto europeo e il coordinamento da parte di ACER. – 4. La gestione delle reti di trasporto e di distribuzione: TSOs, DSOs e *smart grids*. – 5. Progetto pilota di Areti "Romeflex": la flessibilità su base volontaria. – 6. Profili privatistici: tra (etero)integrazione e "conformazione" del contratto. – 7. *Smart contract* e *smart grid*: contratto o algoritmo "normativo"? – 8. La determinazione dell'oggetto ad opera di un soggetto terzo o… di un algoritmo. – 9. Intelligenza artificiale e operazioni economiche: il problema dell'area di rischio consentito. – 10. Conclusioni: dall'interconnessione delle reti alla flessibilità dei contratti su base normativa.

1. Il nuovo *Electricity Market Design* tracciato dall'Ue: tra diritto pubblico e diritto privato

Il 16 luglio 2024 sono entrati in vigore nell'ambito dell'Unione europea due importanti atti normativi che ridisegnano il mercato dell'energia elettrica, precisamente la Direttiva (UE) 2024/1711[1] e il Regolamento (UE) 2024/1747[2]. Essi riformano parzialmente un precedente pacchetto di regole varate nel 2019 e consistenti in quattro atti normativi, dei quali due risultano modificati e riformulati, nella specie la Direttiva 2019/944[3] e il Regolamento 2019/943[4], mentre altri due sono rimasti in vigore nel testo originale ovvero il Regolamento 2019/942[5] istitutivo dell'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia (ACER) e il Regolamento 2019/941[6] sulla preparazione ai rischi nel settore dell'energia elettrica.

L'intervento del legislatore europeo è in linea con l'obiettivo stabilito dall'art. 3 TUE (Trattato

1. Direttiva (UE) 2024/1711 del Parlamento europeo e del Consiglio del 13 giugno 2024 che modifica le direttive (UE) 2018/2001 e (UE) 2019/944 per quanto riguarda il miglioramento dell'assetto del mercato dell'energia elettrica dell'Unione.
2. Regolamento (UE) 2024/1747 del Parlamento europeo e del Consiglio del 13 giugno 2024 che modifica i regolamenti (UE) 2019/942 e (UE) 2019/943 per quanto riguarda il miglioramento dell'assetto del mercato dell'energia elettrica dell'Unione.
3. Direttiva (UE) 2019/944 che ha abrogato la precedente Direttiva 2009/72/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno dell'energia elettrica e che abroga la direttiva 2003/54/CE, Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio del 5 giugno 2019 relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE.
4. Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio del 5 giugno 2019 sul mercato interno dell'energia elettrica, versione consolidata al 16/07/2024.
5. Regolamento (UE) 2019/942 del Parlamento europeo e del Consiglio, del 5 giugno 2019, che istituisce un'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia (rifusione), versione consolidata al 05/02/2025 in e Regolamento (UE) 2024/1106 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica i regolamenti (UE) n. 1227/2011 e (UE) 2019/942 per quanto riguarda il miglioramento della protezione dell'Unione dalla manipolazione del mercato nel mercato dell'energia all'ingrosso.
6. Regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sulla preparazione ai rischi nel settore dell'energia elettrica e che abroga la direttiva 2005/89/CE.

sull'Unione europea) di instaurazione di "un mercato interno" ed in particolare un mercato unico dell'energia in virtù di una competenza generale in materia, stabilita dall'art. 3 Trattato CE come modificato dal Trattato di Maastricht.

In base all'art. 4 TFUE (Trattato sul Funzionamento dell'Unione europea), comma 2, lett. *i*), l'energia rientra tra le materie nelle quali l'Unione esercita la competenza legislativa concorrente, di cui all'art. 2 co. 2 TFUE, e pertanto la recente riforma realizza un ulteriore avanzamento nella direzione dell'instaurazione del mercato interno di cui all'art. 26 TFUE e del perseguimento della coesione economica, sociale e territoriale di cui all'art. 174 TFUE.

Per completezza si ricorda che la definizione di energia è contenuta nella Direttiva 32/2006/CE art. 3, lett. *a*): "qualsiasi forma di energia commercialmente disponibile, inclusi elettricità, gas naturale (compreso il gas naturale liquefatto), e il gas di petrolio liquefatto, qualsiasi combustibile da riscaldamento o raffreddamento, compresi il teleriscaldamento e il teleraffreddamento, carbone e lignite, torba, carburante per autotrazione (ad esclusione del carburante per l'aviazione e di quello per uso marina) e la biomassa quale definita nella direttiva 2001/77/CE del Parlamento europeo e del Consiglio, del 27 settembre 2001, sulla promozione dell'energia elettrica prodotta da fonti energetiche rinnovabili nel mercato interno dell'elettricità".

Per "energia"[7] quale oggetto di attività legislativa degli organi dell'Ue si intende pertanto la "materia concernente le attività connesse alla produzione e alla distribuzione di prodotti energetici"[8].

Oltre agli obiettivi di carattere generale il nuovo modello normativo intende indurre i legislatori e, di conseguenza, gli operatori dei mercati a livello nazionale, a orientarsi verso la scelta di fonti di energia rinnovabile[9] "per raggiungere la neutralità climatica" attraverso l'adozione di forme di regolazione che garantiscano la "sicurezza dell'approvvigionamento, flessibilità, integrazione dei sistemi attraverso molteplici vettori energetici, sostenibilità, decarbonizzazione e innovazione" come esplicitamente enunciato dal nuovo art. 1, lett. *a*) del Regolamento 2019/943.

La principale ed innovativa caratteristica, auspicata ed evidenziata dalla ripetizione del termine, è quella della flessibilità[10] delle formule da adottare per la negoziazione e gestione dei rapporti contrattuali tra "operatori di sistema" – ovvero i TSOs (*Transmission System Operators* o operatori delle reti di trasmissione[11]) e i DSOs (*Distribution System Operators* o operatori delle reti di distribuzione) – e utenti/consumatori, ai quali è richiesto di modulare i termini dell'accordo in base ad esigenze di carattere superiore rispetto a quella della libera contrattazione delle parti, in primo luogo la stabilità e sostenibilità delle reti nella prospettiva della realizzazione della piena interconnessione e interoperabilità delle reti transeuropee di cui agli artt. 170-172 TFUE. Inoltre, l'approvvigionamento, trasporto e distribuzione di energia elettrica

7. Cfr. art. 194 TFUE.
8. Aicardi 2007, pp. 1007-1073, in particolare p. 1007.
9. Per una sintesi della normativa vedasi Marletta 2014, pp. 465 ss.
10. Il termine flessibilità si trova quattro volte complessivamente già nell'art. 1 a seguito della riforma: una volta nella lett. a), due volte nella lett. b) e una volta nella lett. e), aggiunta al testo. Si riporta la lett. b): "Il presente regolamento mira a: […]; b) definire i principi fondamentali di mercati dell'energia elettrica efficienti e integrati, che consentano un accesso non discriminatorio a tutti i fornitori di risorse e ai clienti dell'energia elettrica, favoriscano lo sviluppo di mercati a termine dell'energia elettrica, per consentire ai fornitori e ai consumatori di darsi una copertura o tutelarsi dal rischio di una volatilità futura dei prezzi dell'energia elettrica, responsabilizzino e tutelino i consumatori, assicurino la competitività sul mercato globale, migliorino la sicurezza dell'approvvigionamento e la flessibilità mediante la gestione della domanda, lo stoccaggio di energia e altre soluzioni di flessibilità non fossili, garantiscano l'efficienza energetica, agevolino l'aggregazione della domanda e dell'offerta distribuite e consentano l'integrazione del mercato e del settore e la remunerazione a prezzi di mercato dell'energia elettrica generata da energia rinnovabile".
11. Cfr. Regolamento (UE) 2017/1485 della Commissione del 2 agosto 2017 che stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica.

rientrano tra i servizi di interesse economico generale di cui all'art. 57 TFUE.

Questo studio, come suggerito da autorevoli fonti dottrinarie[12], contempla una pluralità di aspetti, da quello privatistico a quello pubblicistico, compresenti nella materia "energia", presa in considerazione nella duplice prospettiva di risorsa fruibile dal singolo e allo stesso tempo necessariamente funzionale al vivere comune. In realtà i profili da prendere in considerazione sarebbero molteplici poiché la branca del diritto dell'energia nasce dalla "suddivisione per settori operativi"[13] ed appartiene al settore delle materie c.d. "trasversali" poiché "la disciplina di questo oggetto attraversa un po' tutto il diritto sostanziale".

2. L'energia elettrica: da utilità privata a bene pubblico

Sebbene il concetto di energia[14] sia difficilmente inquadrabile nelle rigide cornici del diritto, esso rivendica purtuttavia una legittima collocazione tra le categorie giuridiche. Si ricorda brevemente che per la fisica l'energia è "l'attitudine di un corpo o di un sistema a compiere lavoro"[15], ma il termine ha origine ancor prima della moderna scienza sperimentale nella filosofia greca, come "enérgeia" (ἐνέργεια) o, letteralmente, forza intrinseca, capacità interna di sviluppare un'attività.

Le diverse fonti di energia[16] si trovano in natura e possono essere oggetto di utilizzo, redistribuzione, trasformazione: alcune fonti, come il carbone o gli idrocarburi liquidi o gassosi, sono soggetti a deterioramento e inevitabile consumazione nello stato in cui si trovano, per questo ritenuti non rinnovabili; altre, sono rinnovabili in quanto nuovamente rinvenibili in natura anche dopo il loro utilizzo, almeno sulla base delle (limitate) conoscenze umane all'anno 2025 d.C.

In realtà il primo principio della termodinamica, che vale per tutti i tipi di energia, rivela che essa, nonostante l'apparenza, non è mai distrutta, ma trasformata: quindi da energia termica può tradursi in meccanica, da meccanica in elettrica, ecc. Eppure, l'essere umano non ha ancora sviluppato conoscenze e tecnologie in grado di chiudere "in modo perfetto" il ciclo della rigenerazione energetica, ossia in maniera tale che questo ciclo abbia un'efficienza unitaria e quindi senza che il risultato finale sia uno stato del sistema in cui l'energia complessiva all'inizio del ciclo sia uguale a quella alla fine dello stesso. Per tale ragione ad oggi è impossibile sfruttare a pieno tutte le forme di energia senza dispersioni (i.e., con efficienza unitaria, ossia tale che tutta l'energia venga trasformata in lavoro), anche per la difficile prevedibilità della disponibilità di alcune fonti di energia, che dipendono da condizioni atmosferiche non controllabili dall'uomo come quella eolica, solare, ecc. che impongono lavorazioni, stoccaggi e/o processi aggiuntivi che a loro volta hanno rendimenti inferiori all'unità[17].

Nel tentativo di definire la realtà fisica, sfuggente al giurista, questi si è attenuto non tanto alle qualità sostanziali del fenomeno, bensì alle esigenze dell'economia e del mercato, attente alla regolazione dello sfruttamento, produzione, trasporto e scambio delle risorse energetiche.

12. Cfr. Irti 2004; Di Bona 2008, p. 17. Alessandro Candido parla di "doppio volto dell'energia: merce e servizio di interesse economico generale", cfr. Candido 2011, pp. 87-130, in particolare p. 100.
13. In base a questa "suddivisione delle varie branche del diritto non più per istituti giuridici ma per settori operativi [come] energia, sanità, agricoltura, ambiente, singole attività artigianali e commerciali e così via", chiarisce Federici, "si trova di tutto. Prendiamo il diritto dell'energia: qui abbiamo applicati istituti propri del diritto amministrativo, del diritto penale, del diritto civile e commerciale, del diritto del lavoro, del diritto tributario, del diritto dell'Unione europea…", cfr. Federici 2015, pp. 12-13.
14. Cfr. Calandra 1965, pp. 559-581; Messinetti 1965, pp. 867-875; nonché Pardolesi 1991, pp. 444-448.
15. Del Tin 1987, pp. 393-409.
16. Cfr. sul concetto di energia e la distinzione tra beni energetici e prodotti energetici Federici 2015, pp. 3-13. Per una trattazione giuridico-filosofica in merito al rapporto uomo, risorse energetiche e ambiente cfr. Amato Mangiameli 2021.
17. Troiano 1991, pp. 448-454.

Seguendo un approccio pragmatico, che gli è proprio sin dai tempi del diritto romano[18], il diritto ha dovuto prendere atto dell'utilità[19] fornita da questa realtà fisica e applicare alle attività umane di accesso, approvvigionamento, accumulo, trasporto, utilizzo e scambio di energia le stesse regole elaborate per altre categorie di "beni materiali", anche se solo a titolo analogico[20].

Per questo le energie sono state qualificate come utilità o beni materiali dal codice civile, benché sia stata, e sia ancora, molto discussa l'adeguatezza degli istituti del diritto proprietario a questa particolare specie di beni, non suscettibili di un'effettiva apprensione e appropriazione esclusiva, come invece altre tipologie di beni, materiali o immateriali. Nella direzione della "concretizzazione" del bene "energia", vanno gli sforzi e gli investimenti che tutti i Paesi sostengono nei sistemi di misura (dai comuni "contatori" presenti nelle nostre case ai più evoluti apparati dedicati alle reti elettriche, elementi indispensabili per rendere fruibile un'entità di per sé astratta quale, per l'appunto, l'energia).

Storicamente la grande rivoluzione industriale del XIX secolo rese possibili la distribuzione e l'utilizzo dell'energia elettrica[21] ai fini dell'alimentazione dei meccanismi produttivi su larga scala, mentre per l'uso domestico si dovette attendere ancora qualche decennio.

Da allora la vita individuale e collettiva si è "strutturata" sull'utilizzo di energia elettrica, di talché la sospensione o interruzione di fornitura potrebbe arrecare gravi pregiudizi ad attività di ordine primario dello Stato, come la difesa e la sicurezza, l'incolumità pubblica e la sanità, i trasporti, le telecomunicazioni, l'agricoltura e l'allevamento, la produzione industriale, ecc. Per tali ragioni la gestione delle attività di produzione, trasporto e distribuzione dell'energia elettrica è stata oggetto di nazionalizzazione[22] nel corso del Novecento ed è ormai comunemente intesa e trattata come un "bene essenziale".

In un secondo momento la gestione di quelle attività è stata oggetto di privatizzazione (come si dirà *infra*, par. 3) a causa del mutato quadro normativo e istituzionale in armonia con gli obiettivi dell'unificazione europea: la dottrina ha dovuto ripensare le proprie nomenclature[23] ed allontanarsi sempre più da schemi di tipo proprietario, incardinate sulla titolarità del bene per garantirne la "funzione" pubblica. Da una concezione soggettiva si è passati ad una concezione oggettiva, che qualifica i beni – beni privati vs. beni pubblici – sulla base della loro destinazione, piuttosto che sulla base della natura del soggetto proprietario[24].

Nel tentativo di individuare una categoria intermedia di beni ed una soluzione alla tensione tra interessi privati e pubblici[25], tra sostenibilità economica e fruizione collettiva di alcune risorse non

18. Per un excursus sull'origine della categoria dei beni ad uso pubblico e un'analisi della categoria di beni comuni in dottrina cfr. Sirgiovanni 2017.
19. Pardolesi 1991.
20. L'art. 814 c.c. utilizza infatti l'espressione "Si considerano" a voler sottolineare la qualificazione giuridica che non pregiudica una differente definizione sostanziale: "Si considerano beni mobili le energie naturali che hanno valore economico".
21. Cfr. De Bellis 2006, pp. 2189-2198; nonché Colavecchio 2005, pp. 233-325.
22. Cfr. Landi 1965, pp. 875-913.
23. Cfr. Giannini 1963; nonché Sandulli 1959, pp. 277-300.
24. Renna 2022, pp. 149-181.
25. Tensione che per alcuni è divenuta finanche "tragedia" dinanzi alla "scelta tra opzioni che sono entrambe al contempo vantaggiose e altamente pericolose: l'uso generalizzato del bene ambientale, quale massimizzazione della sua natura oggettivamente pubblica, e la limitazione nell'accesso al bene medesimo, quale strategia per la salvaguardia dello stesso, anche a vantaggio delle generazioni future", cfr. Renna 2022, che si riferisce all'espressione utilizzata come titolo di una pubblicazione dal biologo Garrett Hardin, "The Tragedy of the Commons" pubblicato su Science nel 1968.

escludibili ma rivali[26], è stata elaborata da Elinor Ostrom la nozione di "beni comuni'[27]. Con questa espressione l'economista voleva indicare che per tali entità dovrebbe essere prevista una modalità mista di gestione – modelli di gestione comunitaria – che realizzerebbe il compromesso tra fruizione generalizzata ed efficienza economica. La realizzazione della funzione pubblica non potrebbe essere conseguita né rimettendo la distribuzione ed utilizzo di queste risorse ad una logica di mercato, che non ne garantirebbe l'accesso alla generalità; né ad un regime di monopolio pubblico, come d'altra parte sarebbe inevitabile per gli elevati costi fissi infrastrutturali.

Nonostante i numerosi profili critici della teoria essa risulta utile per individuare un processo di metamorfosi della nozione di bene pubblico, ovvero "una separazione soggettiva, interna alla proprietà pubblica, tra la titolarità del diritto reale sul bene e la titolarità di compiti di gestione e tutela del medesimo. Ciò a conferma del fatto che tale scissione non interferisce con la doverosità, per i soggetti (non proprietari ma) titolari delle prerogative di gestione, dell'utilizzazione dei beni in modo da inverarne efficientemente la gestione pubblica"[28].

Di seguito si comprenderà come il processo di unificazione europea abbia giocato un ruolo decisivo in ordine al mutamento di impostazione della dottrina: essa riservava alle energie dapprima la qualifica di bene pubblico, insistendo sulla concezione soggettiva, in virtù della titolarità in capo allo Stato-soggetto, sullo schema del diritto proprietario. In un secondo tempo, passando attraverso le privatizzazioni degli enti che gestivano queste risorse di pubblica utilità o *public utilities*[29], la scienza giuridica ha dovuto risemantizzare la nozione di bene pubblico in senso oggettivo, valorizzando non più la titolarità del bene ma la sua destinazione o finalizzazione a beneficio della collettività. Per questo le attività economiche, che hanno ad oggetto la produzione, distribuzione, somministrazione di questi beni, sono disciplinate secondo schemi e vincoli tipici del diritto pubblico.

3. Profili giuspubblicistici: il ruolo delle Autorità di regolazione del mercato nel contesto europeo e il coordinamento da parte di ACER

Al fine della realizzazione di un mercato unico dell'energia, negli anni Novanta a seguito del Trattato di Maastricht, sono intervenuti nei diversi Stati membri processi di privatizzazione dei settori di attività "di pubblica utilità nei quali normalmente si realizza un monopolio naturale"[30]: è stato sottolineato che sarebbe stato impossibile realizzare un mercato unico dell'energia sulla base di monopoli pubblici nazionali[31] e pertanto la liberalizzazione costituiva una strada obbligata.

Benché le attività economiche di alcuni settori – tra i quali non solo l'energia, ma anche le telecomunicazioni, ad esempio – siano state oggetto di privatizzazione, tuttavia la rilevanza a livello non solo privato ma anche pubblico degli interessi coinvolti non consentiva di lasciare l'andamento di quei mercati in balia di una logica di libera concorrenza, per due ordini di motivi.

Da un lato, il rilievo pubblicistico era determinato dalla natura stessa del "bene comune'[32] "energia" e dall'interesse diffuso[33] a livello nazionale

26. Questi attributi provengono dal lessico economico per distinguere le diverse categorie di beni, sul punto v. Sirgiovanni 2017, p. 233.
27. Ostrom 1990/2006.
28. Renna 2022, p. 159. Prosegue notando che "quel che maggiormente rileva è che la non coincidenza tra proprietà e gestione risulti sintomatica di una precisa visione di 'pubblicità del bene' fatta propria dal vigente ordinamento, incentrata non più sugli aspetti proprietari, ma su quelli afferenti i profili di valorizzazione e tutela, e dunque, in sintesi, su quelli inerenti alla gestione finalizzata ad inverare la destinazione pubblica del bene medesimo".
29. Cfr. Di Bona 2008, p. 17.
30. Barozzi Reggiani 2020, pp. 221-222.
31. Ranci 2017, pp. 15-56.
32. Cfr. Cerulli Irelli 2016, pp. 529-534; Cerulli Irelli 2022, pp. 639-646; nonché Lucarelli 2021, pp. 21-28, e Marinelli 2014, pp. 157-167.
33. Cfr. Alpa 2014, pp. 349-366.

ad un sistema energetico efficiente[34] e allo stesso tempo rispettoso di altri diritti fondamentali, il cui godimento ed esercizio avrebbe potuto – e potrebbe ancor oggi – essere compromesso da un inefficiente o irregolare sistema energetico (ad es.: diritto alla salute ed alle cure, ad un ambiente salubre, all'iniziativa economica privata, al lavoro, ecc.).

Dall'altro, l'obiettivo dell'unificazione del mercato a livello europeo richiedeva un coordinamento per ciascun settore che non si esplicasse nella logica dei "comitati", funzionanti secondo la modalità tipica delle organizzazioni intergovernative, in quanto costituiti da rappresentanti dei singoli Stati nazionali[35].

La soluzione adottata per il raggiungimento di questi scopi fu l'istituzione a livello nazionale di Autorità amministrative indipendenti[36], formalmente "separate dagli organi di indirizzo politico"[37] – e pertanto non soggette ai mutevoli "venti" della politica – e contemporaneamente in dialogo diretto tra loro a livello transnazionale e con le istituzioni comunitarie tramite un centro di coordinamento a livello europeo.

Questo sistema è finalizzato a perseguire il graduale e progressivo avvicinamento delle posizioni degli organismi amministrativi indipendenti, presenti tramite i loro presidenti nell'organismo di coordinamento europeo, sia nella fase ascendente[38] di supporto alla funzione propositiva della Commissione nell'attività legislativa, sia nella fase discendente della regolazione attuativa delle norme comunitarie.

L'intervento pubblico nell'economia – prima quantomeno correttivo se non "dirigista" – inizialmente accentrato nella figura dello Stato nazionale – è stato sostituito dall'azione delle Autorità amministrative indipendenti, che devono realizzare in determinati settori economici quello stesso contemperamento tra diritto privato e diritto pubblico prima assicurato "dall'alto" e su basi squisitamente tecniche. Queste autorità che, in base alla funzione, possono essere distinte in autorità di garanzia, di vigilanza o regolatorie, devono assicurare o indurre una gestione efficiente in "spazi di mercato privi di barriere e aperti al confronto concorrenziale"[39] e, allo stesso tempo, il rispetto di superiori interessi di carattere pubblicistico, quali: pari condizioni di accessibilità ai servizi; equità dei prezzi; protezione dei diritti degli utenti; rispetto dell'ambiente[40] anche in considerazione delle generazioni future, ecc.

Dato l'iter di graduale redistribuzione di funzioni amministrative all'interno degli Stati nazionali reso indispensabile dal raggiungimento degli obiettivi dell'unificazione del mercato dell'energia, si comprende meglio la funzione dei regolatori dell'Energia elettrica – in Italia[41] dell'ARERA (Autorità per la Regolazione di Energia Reti e Ambiente) – e di un organismo centrale a livello europeo con funzione di "coordinamento reticolare"[42] che garantisca l'uniformità anche nella fase attuativa delle politiche europee, rappresentato dall'ACER (European Union Agency for the Cooperation of Energy Regulators).

4. La gestione delle reti di trasporto e di distribuzione: TSOs, DSOs e *smart grids*

La questione posta al giurista dal nuovo *Electricity Market Design Regulation* riguarda la nuova formulazione dell'offerta di servizi di somministrazione[43] di energia elettrica in conformità ai principi stabiliti dalla disciplina, quali la flessibilità, efficienza e stabilità della rete.

34. Cfr. Gili 2008, pp. 340-353.
35. Cerasoli 2008, pp. 62-95.
36. Cfr. Poto 2008, pp. 54-62; Merusi–Passaro 2002, pp. 143-192. Per una letteratura di respiro internazionale cfr. Baldwin–Cave 1999; Baldwin 1995; Majone 2001, pp. 57-78; Thatcher–Stone Sweet 2002.
37. Cerasoli 2008, p. 66.
38. *Ivi*, p. 68 ss.
39. Barozzi Reggiani 2020, p. 222.
40. Chiariello 2017, pp. 18-47; Cordini 1987, pp. 193-209; Pericu 1987, pp. 189-193; Pozzo 2003, pp. 93-125.
41. Si menzionano, ad esempio, le corrispondenti autorità austriaca E-Control o "Energie-Control Austria für die Regulierung der Elektrizitäts - und Erdgaswirtschaft" nonché la Bundesnetzagentur tedesca.
42. Cerasoli 2008, p. 65.
43. Cfr. Macario–Mazzia 1991, pp. 454-459.

In particolare, il Regolatore nazionale detiene l'importante funzione di attuare la normativa europea traducendola in regole valide nell'ordinamento interno, in modo che quei principi siano non solo calati dall'alto, ma anche assorbiti dagli ingranaggi del mercato.

Ove si debba regolare il mercato dell'elettricità, si deve tenere conto della particolare configurazione di esso sia dal punto di vista infrastrutturale sia da quello gestionale: da questa duplice prospettiva deriva il diverso profilo delle imprese che cooperano all'efficiente funzionamento.

A monte delle attività di trasmissione e distribuzione di energia elettrica si colloca il procedimento amministrativo che si conclude con provvedimento del Ministro dell'Ambiente e della Sicurezza Energetica (MASE) che rilascia la concessione a svolgere le attività di trasmissione o distribuzione di energia elettrica ai sensi dell'art. 1, comma 1 del d.lgs. 79/1999.

Da un lato, i *Transmission System Operators*[44] (TSOs), imprese private – a seguito delle privatizzazioni di cui sopra – che gestiscono e garantiscono il buono stato delle infrastrutture e forniscono il servizio di trasporto dell'energia dalle centrali di produzione ai punti di consegna, fino alle reti di distribuzione. Ben si comprende come questa attività, per l'entità dell'impegno economico, tecnico e gestionale, fosse stata all'origine necessariamente avocata a sé da soggetti pubblici statuali e gestita in regime di monopolio.

Dall'altro lato, i *Distribution System Operators*[45] (DSOs) che, prelevando l'energia dalle reti di trasporto dei TSOs in corrispondenza dei sopra citati punti di consegna, erogano energia elettrica agli utenti finali, imprenditori e consumatori, ai quali offrono il servizio di distribuzione.

Da quanto detto finora emerge la complessità del mercato, che si basa dal punto di vista strutturale sulla cooperazione tra imprese operanti ai diversi livelli di gestione delle infrastrutture di rete e di trasporto dell'energia, nel caso dei TSOs, di distribuzione nel caso dei DSOs; dal punto di vista economico invece, sulla negoziazione e scambio tra produttori, consumatori e *prosumer*[46]. La gestione dei diversi rapporti e interessi ha richiesto l'elaborazione di diversi schemi negoziali o *legal frameworks*, sussumibili finora in tre principali tipologie.

Un primo tipo di contratto è quello di trasporto, concluso dal venditore con TSOs e DSOs, avente ad oggetto il servizio di trasmissione e distribuzione dell'energia al cliente finale.

Il secondo tipo di contratto, utilizzato per la gestione del mercato, è ascrivibile alla categoria dei contratti di servizi e ha ad oggetto la somministrazione di energia elettrica. Da notare che il venditore di energia funge da intermediario tra cliente finale e TSO-DSO, poiché riscuote anche la quota per il servizio di trasporto[47] e distribuzione – oltre all'accisa e l'IVA – e si fa carico di interfacciarsi con il distributore per tutte le problematiche di rete nei confronti del consumatore.

Inoltre, l'impianto del Regolamento 2024/1747 promuove la connessione delle reti transfrontaliere e meccanismi comuni per impedire il sovraccarico

44. I *Transport System Operators* sono rappresentati dinanzi alle Istituzioni europee dalla ENTSO-E – European Network of Transmission System Operators for Electricity.

45. I *Distribution System Operators* sono rappresentati dinanzi alle Istituzioni europee dalla EU DSO Entity – ufficialmente fondata nel giugno 2021 benché previsto già dall'art. 52 del Regolamento (UE) 2019/943 o *Electricity Market Regulation*.

46. *Prosumer*: termine derivante dalla crasi tra produttori e consumatori. In questo lavoro è possibile solo accennare al mercato, all'interno del quale produttori e consumatori scambiano quantità di energia contro corrispettivo: "sul mercato dell'energia elettrica gestito dal GME [ndr: *Gestore dei Mercati Energetici*] (anche noto come *Italian Power Exchange* - IPEX), i produttori e gli acquirenti vendono e acquistano energia elettrica all'ingrosso". Al Gestore dei Mercati Energetici S.p.A. (GME) "è stata inizialmente affidata l'organizzazione e la gestione economica del mercato [ndr: italiano, strettamente collegato a quello europeo] all'ingrosso dell'energia elettrica, nel rispetto dei principi di neutralità, trasparenza, obiettività e concorrenza", cfr. il sito del Gestore.

47. Dalla lettura della fattura emessa dal distributore per erogazione di energia elettrica possono essere estrapolate infatti le voci: "spesa per materia energia", "spesa per il trasporto", "spesa per oneri di sistema", nonché le imposte ed altre partite eventuali. Gli "oneri di sistema" sono "gli importi fatturati per la copertura di costi relativi ad attività di interesse generale per il sistema elettrico, che vengono pagati da tutti i clienti del servizio elettrico", estratto dal sito di ARERA, *Guide e strumenti. Guida alla lettura delle voci di spesa elettricità*.

(o congestione) delle reti o, viceversa, il *black-out*, tramite offerta e acquisto di servizi di regolazione di produzione e consumo di energia, definiti come "servizi ancillari" dalla Direttiva 2019/944[48].

Questa terza categoria di contratti include lo scambio di servizi, diversi dal trasporto e dalla distribuzione dell'energia, consistenti in particolare nel bilanciamento e adeguamento della potenza consumata o prodotta dal singolo impianto in base alle esigenze di stabilità della rete, tramite l'utilizzo di tecniche di accumulo e rilascio, stoccaggio e messa in circolazione, operazioni regolate tramite nuovi dispositivi tecnologici "intelligenti"[49].

Dei tre *legal framework* sopra sommariamente descritti si analizzerà in questa sede solamente il secondo tipo, con particolare riferimento alle novità introdotte dal Regolamento UE 2024/1747.

5. Progetto pilota di Areti "Romeflex": la flessibilità su base volontaria

Il Progetto RomeFlex – "*R*eshaping *O*perational *ME*thods to run grid *FLEX*ibility"[50], presentato ad ARERA il 25 luglio 2023, è stato approvato con delibera 372[51] il 3 agosto 2023, per il primo quadrimestre. Successivamente il Regolamento definitivo con le modifiche al progetto pilota per l'approvvigionamento di servizi ancillari locali proposto dalla società Areti S.p.a., DSO del territorio del Comune di Roma, con l'avvio della seconda fase per il secondo quadrimestre è stato sottoposto all'Autorità con lettera del 14 marzo 2024 ed approvato con delibera 121[52] il 2 aprile 2024.

Il progetto ha pionieristicamente messo in atto i criteri generali stabiliti dalla delibera del 2021 n. 352[53] "per consentire ai DSO di acquisire servizi di flessibilità, compresa la risoluzione delle congestioni nelle loro aree, e incentivarli in tal senso …", in base alla direttiva 2019/944[54] "al fine di gestire e sviluppare in modo più efficiente il sistema di distribuzione".

Tale sperimentazione rientra tra quelle auspicate proprio dalla delibera del 2021 finalizzate a limitare i costi di rinnovo o sostituzione delle infrastrutture: "progetti pilota per l'approvvigionamento di servizi ancillari locali predisposti dalle imprese distributrici (DSO) … prevedendo il coinvolgimento di operatori individuati sulla base di clausole non discriminatorie, che consentano la più ampia partecipazione possibile, nell'ottica della neutralità tecnologica"[55].

In particolare, le specifiche di questi servizi devono essere stabilite di concerto tra DSO, TSO e tutti gli utenti del mercato e devono garantire "la partecipazione effettiva e non discriminatoria di tutti gli

48. Cfr. art. 2 n. 48) della Direttiva 2019/944, che li definisce come servizi "necessari per la gestione di un sistema di trasmissione o di distribuzione compresi il bilanciamento e i servizi ancillari non relativi alla frequenza, ma esclusa la gestione della congestione", cfr. Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio del 5 giugno 2019 relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE. Per comprendere il significato degli oneri di sbilanciamento si veda l'interessante studio di Alessi 2017, pp. 701 ss.
49. Cfr. Maugeri 2020, pp. 13-36.
50. I documenti descrittivi del progetto, in particolare la Relazione tecnica e il Regolamento, sono disponibili alla pagina web di Areti.
51. ARERA, Deliberazione 3 agosto 2023 372/2023/EEL – Approvazione per l'anno 2024, del progetto pilota per l'approvvigionamento di servizi ancillari locali proposto dalla società Areti S.p.a., del "Regolamento del mercato locale della flessibilità" predisposto dal GME e della convenzione-tipo tra GME e imprese di distribuzione per la partecipazione al mercato locale della flessibilità.
52. ARERA, Deliberazione 2 aprile 2024 121/2024/EEL – Approvazione delle modifiche al progetto pilota per l'approvvigionamento di servizi ancillari locali proposto dalla società Areti S.p.a. Il progetto è stato prorogato per il 2025 dalla Delibera ARERA, Deliberazione 17 dicembre 2024 555/2024/R/EEL – Approvazione, per l'anno 2025, del progetto pilota per l'approvvigionamento di servizi ancillari locali proposto dalla società Areti S.p.a.
53. ARERA, Deliberazione 3 agosto 2021 352/2021/R/EEL, Progetti pilota per l'approvvigionamento di servizi ancillari locali.
54. Direttiva 2019/944, v. *supra*
55. ARERA, Deliberazione 3 agosto 2021 352/2021/R/EEL, Progetti pilota …, cit., p. 8.

operatori di mercato, tra cui i soggetti attivi nei servizi di *demand-response*, i gestori degli impianti di stoccaggio dell'energia e gli aggregatori"[56].

La delibera 352/2021 ha tracciato solamente alcune linee direttive per introdurre su base volontaria nel mercato lo scambio di servizi di flessibilità in una prospettiva *demand-response* che prevede determinati requisiti di accesso e una remunerazione equa e uniforme su tutto il territorio nazionale. Sulla stessa linea la 372/2023 ha adottato il medesimo approccio di mercato, lasciando alla libera iniziativa degli operatori e soprattutto dei consumatori la conclusione di contratti flessibili.

Data la proposizione a livello europeo di orizzonti temporali per raggiungere in pochi decenni gli obiettivi della decarbonizzazione e aumento dell'utilizzo di energie rinnovabili[57], si è reso necessario un nuovo quadro regolatorio stabile per consentire la pervasiva diffusione di questi nuovi modelli contrattuali detti "accordi di connessione flessibile".

Tutto questo richiede urgentemente l'interconnessione delle reti e lo scambio di dati[58] tra DSO, TSO e tutti gli utenti per ampliare "l'osservabilità, da parte sia di Terna che dei DSO, dei flussi di energia e dello stato delle risorse sulle reti di distribuzione […] Tale scambio dati contribuisce anche a rendere più efficace il ruolo del DSO come facilitatore neutrale ai fini dell'approvvigionamento dei servizi ancillari globali"[59].

RomeFlex ha l'obiettivo di realizzare il mercato della flessibilità della rete elettrica sul territorio di Roma, permettendo così ai clienti connessi da ARETI di partecipare attivamente alla gestione della rete elettrica e di offrire servizi di flessibilità, contribuendo così a garantire l'equilibrio tra domanda e offerta di energia a beneficio dell'intera comunità territoriale.

Al mercato istituito dal progetto RomeFlex possono partecipare tutti i clienti (definiti dalla delibera 352/2021 *Balance Service Providers* – BSP) che sono in grado di modulare i propri consumi/produzioni, dalle singole utenze da 3kW fino ai grandi impianti di generazione o di consumo che potranno quindi offrire i propri servizi di flessibilità ad Areti sia individualmente che in forma aggregata (anche attraverso comunità energetiche[60]).

Il progetto RomeFlex garantisce l'automazione di tutte le fasi del mercato; grazie all'utilizzo della BlockChain[61] e degli *Smart Contract* è garantita la totale trasparenza e l'immediata certificazione di tutte le transazioni economiche e di rendicontazione tecnica dell'avvenuta fornitura del servizio. I clienti, per aderire al progetto, possono partecipare alle così dette "aste a termine"[62] per fornire flessibilità sul lungo periodo; diversamente possono presentare offerte economiche giornaliere attraverso il cosiddetto "mercato giornaliero a pronti" per risolvere specifiche criticità di rete con condizioni economiche migliorative rispetto a quelle delle aste a termine. In quest'ultima ipotesi gli aggiudicatari delle aste potranno migliorare le condizioni economiche di fornitura per quei determinati orari rispetto a quanto offerto in base d'asta a termine.

Il *market design* implementato dal progetto RomeFlex garantisce la massima efficienza economica e operativa per il sistema elettrico essendo basato su criteri di trasparenza e concorrenzialità a vantaggio di tutti i cittadini che fruiscono di un servizio sempre più stabile e resiliente.

6. Profili privatistici: tra (etero)integrazione e "conformazione" del contratto

Dalla regolamentazione dell'Ue sul mercato dell'energia elettrica deriva l'obbligazione degli Stati

56. ARERA, Deliberazione 3 agosto 2021 352/2021/R/EEL, Progetti pilota …, cit., p. 3.
57. Sulla complessità del processo cfr. Bevilacqua 2024, p. 125 ss.
58. Sulla data economy cfr. Morace Pinelli 2023; Morace Pinelli 2024.
59. ARERA, Deliberazione 3 agosto 2021 352/2021/R/EEL, Progetti pilota …, cit., p. 6.
60. Cfr. sul punto Balestra 2023, pp. 2772-2781; Bartolini 2023, p. 2781 ss.; Di Cerbo 2023, pp. 2749-2761; Favilli 2023, pp. 385 ss.; Ferrero 2020, pp. 677 ss.
61. Sul concetto di Blockchain in generale cfr. Monterossi 2021, pp. 29-38. Per le applicazioni al settore dell'energia Comporti–Lucattini 2020; sull'utilizzo della Blockchain per garantire tracciabilità e verificabilità degli scambi cfr. Bixio 2023, pp. 117-156; Contaldo–Campana 2019. Per un recente studio in prospettiva critica v. Martino–Ringe 2024, pp. 1-29.
62. Cfr. *supra* nota 46.

membri di conformare ai principi di flessibilità, neutralità climatica e aumento dell'utilizzo di energie rinnovabili le normative nazionali di settore.

Come già esposto *supra* al par. 3, grazie alla Commissione, che svolge il ruolo di "server di rete"[63] nella fase ascendente della formulazione di normative settoriali, e grazie alle "strutture reticolari"[64] – costituite dalle Autorità amministrative indipendenti – nella fase discendente, l'uniformazione segue l'iter dell'integrazione amministrativa, molto più agevole, rispetto a quello intergovernativo, e direttamente incisivo sul funzionamento dei mercati.

Seppure carente di legittimazione democratica[65] in senso proprio, la normativa europea di cornice e di dettaglio attuata nei singoli contesti nazionali tramite il canale cosiddetto "sovranazionale-funzionale"[66] – ovvero dai Regolatori in costante dialogo tra di loro e con l'autorità coordinatrice a livello europeo, l'ACER – può incidere direttamente su diritti fondamentali[67] dei cittadini grazie alla legittimazione che le deriva dal suddetto processo di integrazione amministrativa.

Il legislatore europeo può sostituirsi all'autonomia negoziale, imponendo alle imprese un adeguamento a criteri "normativi"[68] – di flessibilità, sostenibilità, ecc. – delle condizioni generali[69] di offerta del servizio di fornitura dell'energia nonché contribuendo a dettare, tramite il potere regolatorio[70] delle Autorità di settore, perfino il contenuto[71] sul quale convergerà l'accordo delle parti.

Da quanto detto la collazione delle clausole del contratto di somministrazione di energia elettrica appare alquanto articolata: esso è soggetto *ab origine* ad un processo di "conformazione"[72] del contenuto alle determinazioni dei Regolatori, che non incidono solo sulla cornice, stabilendo linee guida che indirizzino e coordinino "l'attività economica pubblica e privata … a fini sociali"[73], secondo il

63. La funzione della Commissione è paragonata a quella di "server di rete" da Cerasoli 2008, a p. 71.
64. *Ivi*, p. 69.
65. Per una discussione sul punto si veda Preziosi, il quale nel 2008, in merito alla questione relativa al deficit di legittimazione democratica della legislazione comunitaria, osservava che "in effetti, se la democraticità delle istituzioni viene fondata sulla sovranità e correlata ad essa, difficilmente si potrà riconoscere carattere pienamente democratico alla normazione comunitaria, in quanto questa ha una radice non esclusivamente o non prevalentemente rappresentativa. La legislazione comunitaria […] è di matrice *tecnocratica*" e per questo "… non sembra potersi affrontare da un'unica prospettiva", Preziosi 2008, p. 49 ss.
66. Cfr. sul punto diffusamente Cerasoli 2008, p. 69, e diffusamente nei paragrafi 4, 5 e 7.
67. Cfr. Lillo 2024, nonché Olivetti 2022.
68. Vale a dire che regolano i negozi giuridici utilizzati in quell'area di attività. In questo senso per il settore dell'energia non sono "normativi" i contratti di somministrazione, ma "normati" o "regolati" come osservato da Ferrari, che distingue regolamenti di interessi "privati e regolamenti di fonte autoritativa pubblica" al fine di sciogliere "una significativa commistione tra autonomia privata e prerogative, *lato sensu*, pubblicistiche, in contrasto con la chiarezza del distinguo tra potere conformativo privato e potere conformativo di ascendenza autoritativa", cfr. Ferrari 2018, p. 12. Inoltre, l'autrice chiarisce la differenza tra regolazione attiva e regolazione passiva, che "vede allora il contratto esclusivamente quale oggetto della stessa, stante, dal lato attivo, un regolatore, sempre e comunque diverso dalle parti del contratto regolato, che si colloca in una posizione sovraordinata rispetto ai contraenti", *ivi*, p. 21. Solinas li chiama "amministrati" in Solinas 2018; così anche Prussiani 2022, p. 179 ss.
69. In questa sede non è possibile approfondire la discussione sulla diversa intensità dell'autonomia negoziale delle parti nei contratti conclusi mediante la sottoscrizione di moduli o formulari, predisposti unilateralmente da una delle parti, fattispecie in merito alla quale si rinvia alle trattazioni dottrinarie in materia di condizioni generali di contratto, in particolare vedasi Ambrosoli 2014, pp. 71-91; Morello 1988, pp. 334-397.
70. Cfr. Simeoli 2014, pp. 95-108; nonché Ferrari 2018.
71. Sul punto cfr. Prussiani 2022, p. 98 ss.
72. L'espressione è mutuata da Prussiani 2022. Sullo stesso argomento cfr. Di Bona 2008; nonché Festi 2015, pp. 33-41.
73. È d'obbligo il richiamo all'art. 41 Cost. e al potere pubblico di indirizzo dell'attività economica privata verso "fini sociali", quale deve oggi essere considerato quello della libera concorrenza, sul punto vedasi Azara 2020, p. 194 ss.

dettato costituzionale, ma anche sul disegno interno del negozio.

È interessante osservare a questo punto che la composizione del regolamento contrattuale deriva da una pluralità di fonti.

Considerate come presupposte le norme generali sui contratti ed in particolare quelle sui contratti tra imprenditori (c.d. operatori di sistema) e consumatori[74], la prima fonte delle obbligazioni in ordine gerarchico, procedendo dal generale al particolare, è costituita da norme primarie[75] di carattere pubblicistico, che istituiscono le Autorità amministrative indipendenti e pongono il mercato di riferimento, nel caso di specie quello dell'energia elettrica, sotto il potere regolatorio delle suddette Autorità. La seconda fonte sono le regole prodotte dalle autorità di settore, che incidono direttamente sulla disciplina negoziale in forza del rinvio espresso, contenuto nella norma di ordine primario. Al terzo livello sono interposte le norme sul contratto tipico, quello di somministrazione, nel caso di specie; mentre l'ultima fonte è l'autonomia privata.

La disciplina contrattuale – frutto di una negoziazione che per sua natura vede tre parti coinvolte, ossia l'erogatore del servizio, il fruitore del servizio ed un ente terzo di controllo – è composta pertanto da una cornice esterna, dettata da fonti diverse dall'autonomia delle parti – a tutela di interessi pubblici o "fini sociali", di categorie produttive o del contraente più debole – ed una minima parte, ridotta finanche alla mera adesione, posta dall'autonomia dei contraenti.

L'ARERA ha infatti predisposto un modello di contratto, quasi un "contratto-quadro", che riassume la normativa primaria e secondaria di obbligatoria adozione, quale modello valido per un numero indefinito di casi, denominato "Codice di rete per il servizio di trasporto dell'energia elettrica"[76].

Ma vi è di più. La normativa primaria, comprensiva delle norme istitutive delle Autorità e delle norme sul contratto-tipo, e le norme secondarie del potere regolatorio pubblico "conformano" non solo le condizioni generali di contratto, a garanzia del buon andamento del mercato e dell'utilità sociale[77] – nel rispetto di principi generali di trasparenza dell'offerta, equità dei prezzi, concorrenza leale, ecc. –, ma anche l'oggetto[78] – quindi la determinazione della qualità e quantità, potenza, orari e limiti della fornitura di energia – che deve adeguarsi tramite un algoritmo alle mutevoli condizioni della rete e quindi essere flessibile o costantemente rideterminato. L'autonomia privata in questo caso non ha potere di dettare le regole, ma solo di approvarne ed assumerne il contenuto nella sfera soggettiva di interessi, oppure no.

7. *Smart contract* e *smart grid*: contratto o algoritmo "normativo"?

Il nuovo *Electricity Market Design* pone un quesito giuridico, nella misura in cui richiede la

74. I contratti di somministrazione di energia elettrica rientrano nell'ampia categoria dei contratti tra imprese e consumatori, negozi nei quali si manifesterebbe un palese squilibrio di forza contrattuale tra le parti, se il diritto non intervenisse a correggere le posizioni e bilanciare le prestazioni corrispettive per evitare che la parte debole non abbia altra scelta che accettare condizioni eccessivamente onerose, oppure non usufruire affatto del servizio. Cfr. Antoniolli 2011, pp. 208-238; nonché Gabrielli 2006, pp. 227-268.

75. Azara 2020. L'autore ricostruisce il meccanismo di integrazione del contratto *ex* art. 1374 c.c. anche da parte di norme secondarie, non menzionate dall'articolo suddetto come fonte di integrazione, tramite il richiamo, purché espresso, da parte della fonte primaria speciale, che legittima il potere regolatorio dell'Autorità amministrativa indipendente.

76. Si tratta di un documento frutto del lavoro di un gruppo costituito da Terna, rappresentanti di DSOs e utenti finali, cfr. ARERA, *Codice di rete tipo per il servizio di trasporto dell'energia elettrica. Fatturazione del servizio e garanzie contrattuali. Orientamenti finali, Documento per la consultazione 263/2014/eel in*. In qualche modo questo testo esplica la stessa funzione di un "contratto normativo", benché il fatto che sia emanato da un'autorità pubblica escluda la natura contrattuale. Per il contratto normativo cfr. Salvadori 1995, pp. 169-230; Fercia 2013, pp. 194-207.

77. Art. 41, co. 3 Cost.

78. Cfr. Gabrielli 2001, p. 15 ss.; Gabrielli 2004, pp. 328-329; Gabrielli 2009, p. 905 ss.

formulazione di nuovi *legal frameworks* "conformati" ai parametri enunciati in astratto dagli atti normativi europei del c.d. pacchetto "Unione dell'energia"[79].

Per il giurista la questione si traduce ulteriormente nell'elaborazione di istruzioni precise per la stesura del contenuto del contratto e del codice informatico[80] – laddove la determinazione delle prestazioni contrattuali sia gestita attraverso strumenti informatici[81] quali, ad esempio, gli *smart contract*[82] – affinché in fase di esecuzione siano garantiti non solo l'esatto adempimento e l'equo bilanciamento dei rispettivi interessi delle parti, in un contratto che rimane "*b2c*"[83], ma anche la realizzabilità e, per così dire, la "sostenibilità tecnica" delle prestazioni anche in caso di variazioni delle condizioni della rete.

Nel regolamento di interessi dovrà infatti essere riportato che la prestazione del somministratore di energia elettrica sarà modulata costantemente da una funzione che riduce, aumenta o addirittura interrompe la potenza dell'erogazione al singolo utente, in base ad esigenze tecniche di stabilità ed equilibrio della rete locale di distribuzione o della rete di trasmissione. L'accordo, dunque, deve ricomprendere nel suo contenuto anche un algoritmo, che si potrebbe qualificare "normativo" o regolatorio, in quanto stabilisce le regole in base alle quali la prestazione del fornitore varia, al variare delle condizioni della rete.

Questa funzione dovrebbe evitare i congestionamenti o i *blackout* del sistema, tenendo conto di alcuni dati invariabili e l'andamento di alcune variabili dipendenti: data la capacità della rete di distribuzione in quella porzione territoriale, si dovrà garantire che l'energia immessa da tutti i produttori-imprenditori e *prosumer* – quindi da tutte le plurime fonti[84] di produzione laddove esistenti: impianti solari, pale eoliche, ecc. – e quella domandata dagli utenti collegati alla rete con i rispettivi impianti – serviti dallo stesso o da diversi distributori – siano in permanente equilibrio.

Concetti normalmente estranei alla riflessione giuridica in materia negoziale, quali l'efficienza tecnica e la sostenibilità dell'erogazione di un servizio, sembrano reclamare un ruolo, come parametri di valutazione dell'esatto adempimento o della corrispettività delle prestazioni. Nel nuovo sinallagma, infatti, il (contrap)peso delle obbligazioni non può essere fissato una volta per tutte, ma deve essere continuamente ricalcolato sulla base di plurime variabili, dalle quali dipende la stabilità e il buon funzionamento della rete.

79. Cfr. COM (2015)80 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank "A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy". Nel 2018 è stato approvato il Regolamento (UE) 2018/1999 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 sulla governance dell'unione dell'energia e dell'azione per il clima, e nella versione consolidata del 20/11/2023.
80. Sul tema vedasi Sirgiovanni 2023, pp. 214-226 e Sirgiovanni 2022, pp. 415-427.
81. Cfr. Iaselli 2022; Amato 2020, p. 1259 ss.; nonché Benedetti 2021, pp. 412-426; Marone 2022, pp. 669-678.
82. Si ricorda che la nozione di *smart contract* non è propriamente traducibile come contratto intelligente, poiché la dottrina ha chiarito che l'esecuzione del codice informatico non coincide con l'esecuzione del contratto. Più che un contratto il c.d. *smart contract* è un "protocollo idoneo a rendere automatica l'esecuzione del contratto", cfr. Maugeri 2020, pp. 13-36. In generale sulla definizione di *smart contract* v. anche Cerrato 2020, p. 378 ss.; e Janssen–Patti 2020, pp. 31-50.
83. La species contratto di somministrazione di energia si inserisce nel più ampio *genus* dei contratti tra imprenditore e consumatore o "*business to consumer*" (abbreviato *b2c*) oppure addirittura in quello di un "quarto contratto" per gli "scambi che si realizzano nei mercati sottoposti a regolazione amministrativa". Questa ultima categoria si aggiungerebbe ad "un "terzo contratto" (sintetizzato nell'acronimo *b2b*) […] , dopo il "primo contratto" che sarebbe quello a cui si riferisce il Codice civile, e dopo il c.d. "secondo contratto" (*b2c*) …" anche se tale nomenclatura non potrebbe che avere solo valore descrittivo, a pena di uno svuotamento della nozione stessa di contratto in generale, cfr. D'Amico 2023, p. 418 in nota. Vedi anche Oppo 2006, pp. 665-676; Scognamiglio 2006, pp. 851-868.
84. Sulle altre fonti di energia Vitucci 1991, pp. 459-468; nonché D'Addezio 2018, pp. 1-25.

L'intelligenza di rete, ossia l'insieme degli algoritmi informatici che ne regolano il funzionamento, entra nella fase di esecuzione del contratto tramite un protocollo informatico che rende automatico l'adeguamento della prestazione alle condizioni della rete. Le *smart grid*, attraverso la costante controllabilità e comunicabilità dei dati relativi alla produzione e al consumo di energia da parte delle diverse unità connesse per mezzo di *smart meter*, rendono possibile l'automatico adeguamento dell'erogazione, e quindi della prestazione del somministratore, alle condizioni tecniche della rete stessa.

Si può quindi concretamente formulare un nuovo contratto "flessibile" concluso tra un DSO e un consumatore, nel quale sia previsto dalle pattuizioni *ab initio* che la somministrazione di energia elettrica sia automaticamente ridotta o interrotta in prestabiliti periodi dell'anno o orari del giorno, ove sia richiesto dalla stabilità della rete, monitorata da dispositivi di osservazione e controllo; ma anche che essa possa variare, durante l'esecuzione continuata, in base alle determinazioni di un algoritmo (in futuro sempre più basati sull'intelligenza artificiale).

8. La determinazione dell'oggetto ad opera di un soggetto terzo o… di un algoritmo

L'innovazione tecnologica introdotta dall'*Electricity Market Design Regulation* si riverbera quindi nell'architettura giuridica "flessibile" dei contratti, non tanto con riguardo alla "cornice", secondo quanto detto *supra*, ma con riguardo all'oggetto.

Sembra singolare che l'oggetto del contratto sia determinato di volta in volta da un algoritmo, che perciò dovrebbe essere quantomeno menzionato, se non analiticamente descritto nel contenuto[85], eppure apparentemente è l'unica ricostruzione per preservare, da un lato, la validità del consenso, che deve riguardare un assetto di interessi definito e, dall'altro, la "possibilità" dell'oggetto, e quindi delle prestazioni, trasformatasi in efficiente "*performance* tecnologica".

In base alla definizione dell'articolo 1321 c.c. e alla successiva disposizione dell'articolo 1325 c.c., infatti, l'oggetto è uno degli elementi costitutivi[86] del contratto, insieme all'accordo, alla causa e alla forma, quando è prevista *ad substantiam*.

Se è vero quanto detto sinora, ovvero che il regolamento contrattuale dei nuovi *legal framework* del mercato energetico include un "algoritmo", allora l'accordo – quindi il consenso su un preciso regolamento di interessi – dovrà esplicitamente comprendere e contemplare anche quest'ultimo.

Infatti, non è l'algoritmo a "contenere" il regolamento contrattuale – come apparentemente farebbe pensare il concetto di "versamento" dei termini del contratto nel linguaggio informatico – ma viceversa è il regolamento contrattuale che contiene[87] un algoritmo, e precisamente lo "nomina" nella qualità di terzo, agente intelligente, che determina l'oggetto[88], inteso come entità della prestazione.

Se l'algoritmo sostituisce il "terzo" ai sensi dell'art. 1349 c.c. del contratto, allora questo meccanismo deve essere trasparente, conosciuto o almeno conoscibile dalle parti, affinché possano essere salvaguardate l'autonomia del consenso e la consapevolezza, e quindi la comprensibilità, se non la comprensione, del contenuto sul quale esso si esprime.

Si potrebbe perfino ipotizzare un'integrazione all'art. 1346 c.c. che dovrebbe contemplare l'ipotesi dei contratti ad oggetto "flessibile", oltre a quelli ad oggetto "possibile, determinato o determinabile", proprio perché la determinazione non avviene una volta per tutte.

Questo discorso si intreccia con la nozione di *smart contract*, alla quale si accennava *supra* e che richiede un chiarimento anche in funzione dell'ascrivibilità, o meno, dei contratti "flessibili" a questa categoria.

85. Cfr. Prussiani 2022, pp. 109-113.

86. Per una analisi degli elementi del contratto cfr. Cataudella 2019.

87. Nell'ampia discussione dottrinale sull'oggetto del contratto emergono le divergenti tendenze a sottolinearne la realtà di "termine di riferimento esterno" o al contrario la sua ricomprensione all'interno del contenuto, Gitti 2006-a, pp. 355-390, in particolare p. 367. In dottrina Fiori 2003, pp. 169-238.

88. Cfr. *supra* nota 75.

La nozione stessa di *smart contract*, infatti, non è univoca in dottrina[89] e con essa si può indicare alternativamente "protocolli di transazione che possono riguardare la fase di conclusione ed esecuzione di un contratto, solo di esecuzione di un contratto o anche esecuzione di protocolli che nulla hanno a che fare con il contratto"[90].

Alcuni autori lo usano per indicare solo i protocolli che girano su DLT[91], *Distributed Ledger Technologies*, e che prevedono sia la descrizione dello scambio che l'esecuzione dello stesso, mentre altri ammettono un'accezione più ampia.

Secondo un'autorevole classificazione, per creare un minimo di ordine, gli *Smart legal contract*[92] sono quelli che girano su DLT e consentono sia la conclusione della transazione che l'esecuzione; mentre gli altri protocolli sono denominati *Smart code contract*. La fondamentale differenza sta nel fatto che l'esecuzione dei contratti che girano su piattaforme DLT è sottratta alla volontà dei contraenti, mentre l'esecuzione di quelli che girano su piattaforme proprietarie può sempre essere interrotta, appunto, da chi ne è proprietario.

Non potendosi in questa sede approfondire oltre l'interessante argomento, si mutua l'espressione *smart contract* nella limitata accezione di protocollo idoneo ad eseguire in modo automatizzato un contratto[93], e pertanto come codice[94] piuttosto che come contratto in senso proprio.

Collegando i due discorsi, se l'adempimento è automatizzato e sottratto ad atti dispositivi di entrambe le parti allora non solo è escluso l'inadempimento[95], ma ci si trova davanti ad una nuova modalità esecutiva del contratto.

Infatti una volta che l'agente software[96] o sistema di IA[97] abbia determinato l'entità della prestazione, questa, attraverso il protocollo informatico *smart*, sarà eseguita automaticamente nella misura indicata dall'algoritmo[98].

L'automatizzazione[99] dell'esecuzione, tuttavia, apre ulteriori scenari problematici[100]: affinché non si verifichi in fase di esecuzione il rischio di una sopravvenuta maggiore onerosità per una delle parti e quindi uno squilibrio delle prestazioni contrattuali corrispettive[101], tale da far saltare l'equilibrio[102] del sinallagma ponderato inizialmente,

89. Cfr. nota 79. In dottrina cfr. Di Ciommo 2019; Maugeri 2021; nonché Salito 2019. Vedasi anche European Commission 2021; e EU Blockchain Observatory and Forum Experts Panel 2022.

90. Maugeri 2021-a, p. 29.

91. La DLT è "una tecnologia che consente la registrazione e la conservazione di dati attraverso archivi multipli (ledger) ognuno dei quali contiene contemporaneamente gli stessi dati che sono conservati e controllati da una rete di computer (nodi)", cfr. Maugeri 2021-a, p. 28. Per una ricostruzione della disciplina italiana e comunitaria in materia di DLT cfr. Lener 2023, pp. 376-387. L'origine delle monete virtuali è fatta risalire a Nakamoto 2008.

92. In Maugeri 2021-a, p. 33.

93. Questa ricostruzione è coerente con l'assunto che la diffusione degli *smart contract* non potrà soppiantare l'articolato sistema di norme sui contratti, Werbach–Cornell 2017, pp. 313-382.

94. Secondo la classificazione di Maugeri sarebbero *Smart code contract*, in Maugeri 2021-a, p. 33.

95. Sull'esclusione dell'inadempimento e l'automatismo della esecuzione come principali caratteristiche degli *smart contract* che girano su DLT cfr. Maugeri 2021-a, p. 24: "… in altre parole, affidando alla DLT la conclusione dell'accordo e l'esecuzione dello stesso, si impedisce l'inadempimento perché l'uomo non può intervenire per bloccare l'esecuzione".

96. Gallo 2022, pp. 1-3.

97. Rangone 2023, pp. 749-776.

98. Vedasi Maugeri 2021-a, p. 79 ss. per alcuni esempi di "utilizzo di DLT e *Smart Contracts* nel settore dell'energia" come il sistema di "Enerchain … [messo] a punto da Ponton, una società con sede ad Amburgo" e quello di "Power Ledger, una società australiana".

99. Romeo 2024, pp. 5-18; Spatuzzi 2023, pp. 406-413.

100. Su alcuni aspetti problematici dell'utilizzo degli *smart contract* cfr. Vatiero 2022.

101. Sul contratto bilaterale e contratto con prestazioni corrispettive cfr. Cataudella 1998, pp. 31-42.

102. Sul rischio nei contratti d'impresa aventi ad oggetto prestazioni periodiche o continuative di cose – come i contratti di somministrazione di energia, per i quali sussista una fonte extracontrattuale di determinazione

sarà necessario prevedere nuovi rimedi, che prevengano oppure tutelino l'utente dinanzi a possibili deviazioni o malfunzionamenti[103] dell'algoritmo. Da un lato interventi correttivi *ex post*, in particolare la possibilità di valutare la non arbitrarietà della determinazione del terzo; dall'altro strumenti che *ex ante* stabiliscano "paletti" normativi[104], tradotti in linguaggio informatico, all'algoritmo.

9. Intelligenza artificiale e operazioni economiche: il problema dell'area di rischio consentito

A questo punto è "necessario interrogarsi sulla compatibilità delle discipline generali con le *nuove tecnologie*, che modificano in modo significativo l'organizzazione dello scambio economico"[105]. Nell'accordo di connessione flessibile la "sostituzione della tecnica all'uomo"[106] non si verifica nella fase della formazione del contratto – nella quale pure può giocare un ruolo strumentale – ma nella fase esecutiva. Peraltro, la etero-determinazione (almeno nella gran parte) del contenuto non inficia il consenso, che è atto dispositivo dei propri diritti ed interessi da parte del soggetto-consumatore, il quale è consapevole dei diritti e obblighi che assume o che accetta di assumere subordinatamente al verificarsi di determinate condizioni[107] della rete. Tuttavia, rimane il dubbio[108] che in mancanza di una reale trasparenza[109] e comprensibilità[110] dell'algoritmo, il consenso[111] delle parti possa risultare viziato, perché l'adesione al contenuto del contratto e dell'algoritmo farebbe sorgere

dell'oggetto – che possa sorgere un'obbligazione di eseguire una prestazione di entità "discrezionale", in assenza di parametri massimi e minimi richiesti dall'art. 1560, 2° comma c.c per salvare il contratto dall'ipotesi di "nullità per indeterminatezza dell'oggetto" cfr. Gitti 2006-a, in particolare p. 387.

103. Per il problema dei bias, qui solo accennato, cfr. Abriani–Schneider 2021, pp. 38-42.

104. Sul complesso rapporto tra Intelligenza artificiale e diritto cfr. Amato Mangiameli 2023, pp. 275-280; Amato Mangiameli 2022, pp. 213-225; Amato Mangiameli 2017, pp. 147-167; Finocchiaro 2022, pp. 1085-1099; Gabrielli–Ruffolo 2019, p. 1657 ss.; Sartor 2022.

105. Maugeri 2021-a, p. 19. In merito all'impatto delle nuove tecnologie sull'economia e sulla relativa regolazione da parte del diritto cfr. Abriani 2022, pp. 743-765; Gabrielli 2009, p. 905 ss.; Moro Visconti 2024, pp. 45-57; Nuzzo 2022, p. 417 ss.

106. Sirgiovanni 2023, p. 216; nello stesso senso il saggio di Werbach–Cornell 2017.

107. Lo *smart contract* può assumere la funzione di "bloccare la somministrazione in caso di mancato pagamento delle bollette" cfr. Marchetti 2022, p. 126 in nota.

108. Sulla problematica dell'incidenza della tecnologia sui diritti individuali senza una vera e propria legittimazione cfr. Simoncini 2019, pp. 63-89.

109. Ai sette principi guida per un'IA affidabile fa espresso riferimento il considerando 27 del recente AI Act (Regolamento (UE) 2024/1689): "Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. […] Secondo gli orientamenti dell'AI HLEG con 'intervento e sorveglianza umani' si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia". Per i documenti del Gruppo europeo di esperti sull'IA vedi, *infra*, i riferimenti bibliografici. Nell'ambito delle Nazioni Unite cfr. UNESCO 2021. In dottrina, *ex multis*, Lucarelli Tonini 2023, pp. 327-362.

110. Sull'*explainability* dell'intelligenza artificiale Messina 2023, la quale distingue tra opacità tecnica, giuridica e intrinseca, essendo quest'ultima: "un fenomeno che si manifesta allorquando è la macchina a dettare autonomamente la regola, rendendo di fatto inaccessibile, anche agli stessi programmatori, l'iter che conduce all'esito dell'elaborazione delle informazioni", pp. 279-280.

111. Gentili 2022, pp. 701 ss.; Imbruglia 2023, p. 921 ss.

nella sfera soggettiva di interessi non solo diritti, ma anche obblighi in misura non pre-determinata e non pre-determinabile[112].

Nella nuova fattispecie non appare tanto problematico l'automatismo nell'esecuzione – similmente a quanto accade nei contratti condizionati – quanto la variabilità dell'entità delle prestazioni del somministrante e dei diritti del somministrato a rischio di nullità per indeterminatezza dell'oggetto e perciò una certa alea, che renderebbe paragonabili i contratti in parola ai contratti di rischio[113] o, appunto, aleatori.

L'unica via d'uscita da quest'impasse – della dubbia validità in linea di principio di un consenso espresso su un regolamento di interessi almeno in parte "opaco", che sarà completato da un agente software – può essere trovata nella chiarezza dei valori-limite *in melius* o *in peius* delle fluttuazioni, che le prestazioni dei somministratori o i diritti degli utenti possono subire, rispettando il dettato dell'art. 1560, 2° e 3° comma c.c.: discorso senz'altro valido per le negoziazioni nei mercati non regolamentati.

Tuttavia, la natura pubblicistica degli interessi sottesi alla regolazione del settore economico in oggetto consente di controbilanciare il sacrificio dell'interesse del singolo e del diritto alla prestazione – non più rispondente al criterio del "fabbisogno" normale o del "minimo" prestabilito ai sensi dell'art. 1560 3° comma c.c. – con il peso superiore di quello alla sussistenza e funzionamento della rete elettrica. Sui piatti della bilancia non sono posti solo due interessi di natura privata, quello dell'impresa alla gestione economica dell'attività e quello del consumatore all'accesso ed utilizzo a condizioni eque del servizio, ma anche un interesse pubblico, che l'*Authority*[114] è legittimata a proteggere – riequilibrando le prestazioni – o perfino a far prevalere a costo della compressione dei diritti dei singoli, fino al limite di un vero e proprio annichilimento o "espropriazione" per pubblica utilità del potere privatistico di negoziazione e quindi del declassamento dei diritti soggettivi ad interessi legittimi.

Questo meccanismo legittima l'algoritmo, che svolge la funzione di determinazione dell'oggetto, a modificare l'entità delle prestazioni in modo potestativo, unilaterale, bypassando le normali valutazioni di corrispettività, bilanciamento ed eccessiva onerosità delle prestazioni senza che l'output – i.e., la determinazione dell'entità della prestazione, ivi compresa l'interruzione di fornitura – possa essere assoggettata ad un giudizio di arbitrarietà o vessatorietà, se tale "flessibilità" è richiesta dalla stabilità della rete.

Nel mercato dell'energia elettrica, in base alla nuova disciplina del mercato, il limite tecnologico dell'infrastruttura energetica diventa architettura legale o *legal design*[115], che giustifica l'imposizione[116] autoritativa al privato di un'alea significativa di espropriazione dei propri diritti in considerazione del pubblico interesse[117].

La triade impresa-utente-authority partecipa non solo alla fase di formulazione o "configurazione"[118] del contenuto del contratto, ma anche, in qualche modo, alla fase di esecuzione, poiché l'autorità regolatrice, garante di interessi pubblici di rango superiore, dovrà anche monitorare eventuali effetti distorsivi, prodotti dagli algoritmi, sulle

112. Sulla "distinzione tra contratti civili ad oggetto determinato e contratti commerciali ad oggetto determinabile" cfr. Gitti 2006-a, p. 376 ss.

113. In particolare sull'accettazione di un'area di rischio di imprevedibilità dell'output da parte di chi utilizzi sistemi di IA capaci di decisione autonoma, benché più diffusamente e in un orizzonte di discussione ben più ampio, vedasi cfr. Preziosi 2022, p. 720.

114. Contessa 2024, pp. 25-48.

115. Cerrato–Culasso–Crocco 2023, pp. 371-414.

116. Con riferimento al contenuto "imposto" vedasi Prussiani 2022, pp. 57-120.

117. Sulla intersezione tra Intelligenza artificiale e perseguimento della sostenibilità e della tutela dell'ambiente cfr. Pirozzoli 2024, pp. 109-120.

118. Con riferimento al ruolo "configurativo" del contratto vedasi Palermo 1991, p. 109 ss., il quale tuttavia lo costruisce con riguardo al potere regolatorio dell'autonomia privata e non di enti di natura pubblicistica.

condizioni di erogazione del servizio e quindi sul funzionamento della rete e del mercato[119].

10. Conclusioni: dall'interconnessione delle reti alla flessibilità dei contratti su base normativa

Nel più ampio orizzonte delle "transizioni"[120] alle quali l'Unione europea[121] invita i cittadini, quella energetica occupa un ruolo rilevante. In particolare, la normativa esaminata non si limita a regolare uno specifico settore produttivo ma è idonea a incidere direttamente su diritti individuali dei singoli.

Nella configurazione dei contratti del mercato dell'energia elettrica il passaggio da un'adesione ai contratti flessibili volontaria, remunerata e basata sul principio demand/response, come nel caso di RomeFlex, ad un modello di contratto "imposto" nella quasi totalità del contenuto, comprensivo di un'area di rischio di limitazione dei diritti individuali, non appare di poco conto.

Questi nuovi regolamenti contrattuali "codici di rete europei della flessibilità / demand response"[122]sono allo studio di ACER, che ha coinvolto in una consultazione pubblica conclusasi lo scorso 31 ottobre 2024 i principali stakeholders, attori istituzionali e operatori di mercato.

Possiamo prevedere che la completa implementazione in Europa ed in Italia dei contratti flessibili si avrà con l'approvazione dei relativi codici di rete da parte dell'ACER (prevista per il Q3 2025) ed il successivo recepimento in Italia da parte dell'ARERA, previsto per il 2026.

I fornitori di servizi di distribuzione di energia elettrica (DSOs) in base alla nuova normativa dovranno adeguare nel corso dei prossimi anni i modelli di contratto di somministrazione di servizi al requisito della flessibilità, per realizzare non solo la funzione economico-sociale dello scambio tra erogazione di energia elettrica e corrispettivo, ma anche assicurare la stabilità delle reti, l'efficienza tecnologica e l'aumento delle energie rinnovabili.

In questo settore non si integrano solo diritto pubblico e privato, nella misura in cui l'interesse privatistico deve adeguarsi a criteri di equità di distribuzione delle risorse (giustizia distributiva), parità di accesso ai servizi e ai beni comuni (diritto pubblico soggettivo), tutela dei diritti dei consumatori (giustizia commutativa, diritto privato); ma anche diritto e tecnica[123], infrastrutture giuridiche e infrastrutture tecnologiche che rendono labile il confine tra fattibilità e legittimità, possibilità giuridica e sostenibilità tecnica.

Gli obiettivi stabiliti dal *Clean Energy Package*[124], in primo luogo della decarbonizzazione e della neutralità climatica, sono calati nella regolazione del mercato del settore energetico tramite l'enunciazione di principi – di cui all'art. 1 del Regolamento 2019/943, come modificato dal Regolamento 2024/1747 – che informano le norme

119. Sull'integrità del mercato come bene giuridico tutelato anche dal diritto penale cfr. Preziosi 2008, p. 202 ss.

120. Vedasi ora il contratto di interconnessione in Pace 2007, pp. 353-374. Per uno studio sull'implementazione delle energie rinnovabili nel contesto urbano cfr. Pergolizzi 2021, pp. 107-131.

121. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni il green deal europeo COM(2019) 640. Già nel 2007 era stato emanato "Un piano strategico europeo per le tecnologie energetiche (piano SET) – Verso un futuro a bassa emissione di carbonio", cfr. COM(2007) 723: Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 22 novembre 2007.

122. Cfr. la documentazione in merito alla Consultazione pubblica aperta da ACER il 5 settembre 2024 e conclusasi il 31 ottobre 2024 sulla proposta di codice di rete europeo della flessibilità *demand/response*, ACER, *Public consultation on Demand Response Network Code*.

123. Cfr. Preziosi 2022, p. 721 sulla dialettica tra diritto e tecnica.

124. Cfr. Regolamento (UE) 2021/1119 del Parlamento europeo e del Consiglio del 30 giugno 2021 che istituisce il quadro per il conseguimento della neutralità climatica e che modifica il regolamento (CE) n. 401/2009 e il Regolamento (UE) 2018/1999, "Normativa europea sul clima", e lo studio European Commission, Directorate-General for Energy, *Clean energy for all Europeans*, Publications Office, 2019.

settoriali e nazionali e per effetto di queste integrano[125] la disciplina contrattuale.

La flessibilità, enunciata al suddetto art. 1 e definita dal n. 79 dell'art. 2 novellato come "la capacità di un sistema elettrico di adattarsi alla variabilità dei modi di generazione e consumo e alla disponibilità della rete nei diversi orizzonti temporali del mercato", da condizione strutturale del sistema energetico diventa attributo del contratto o, più precisamente, dell'oggetto del contratto.

Se il "goal" è la decarbonizzazione, la *smartness* delle reti elettriche è una pre-condizione o una "skill" del sistema, misurabile sulla base dei parametri illustrati nel documento *Smart Grid Key Performance Indicators: a DSO perspective*[126], che permette di realizzare la flessibilità dell'erogazione di energia elettrica in uno scenario che comprende una pluralità di soggetti generatori, distributori e consumatori, che interagiscono grazie all'intermediazione di un Gestore del Mercato Elettrico, che sovrintende alla certezza delle transazioni sulla base della legge della domanda e dell'offerta.

Il recepimento di quei principi enunciati dalla riforma da parte degli operatori economici si gioca adesso sul campo della regolazione di settore a livello di coordinamento europeo e nazionale, nonché sulla base della assunzione di responsabilità o *awareness* dei cittadini europei, più o meno disposti ad accettare limitazioni o variazioni delle loro abitudini di approvvigionamento e consumo di risorse energetiche nella consapevolezza di contribuire al "bene comune"[127].

Riferimenti bibliografici

Aa.Vv. (2006), *Studi in onore di C.M. Bianca*, tomo III, Giuffrè, 2006

Aa.Vv. (2015), *Dialoghi sul diritto dell'energia*, vol. II, *Contratti dell'energia e regolazione*, Giappichelli, 2015

N. Abriani (2022), *Le categorie della moderna cibernetica societaria tra algoritmi e androritmi: "fine" della società e "fini" degli strumenti tecnologici*, in "Giurisprudenza commerciale", 2022, n. 5

N. Abriani, G. Schneider (2021), *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, il Mulino, 2021

N. Aicardi (2007), *Energia*, in M.P. Chiti, G. Greco (a cura di), "Trattato di diritto amministrativo europeo", parte speciale, tomo II, Giuffrè, 2007

R. Alessi (2017), *Distribuzione di energia elettrica e oneri di sbilanciamento: un caso emblematico di difficile compatibilità tra diritti dei consumatori e regole di mercato*, in "Europa e Diritto privato", 2017, n. 1

G. Alpa (2014), *Interessi diffusi*, in "Digesto delle Discipline Privatistiche", Sezione Civile, agg. I, UTET, 2014

C. Amato (2020), *La 'computerizzazione' del contratto (*Smart, data oriented, computable *e* self-driving contracts. *Una panoramica)*, in "Europa e diritto privato", 2020, n. 4

A.C. Amato Mangiameli (2023), *Intelligenza artificiale*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023

A.C. Amato Mangiameli (2022), *Intelligenza artificiale*, in E. Sgreccia, A. Tarantino (diretto da), "Enciclopedia di Bioetica e Scienza Giuridica", agg. vol. I, Edizioni Scientifiche Italiane, 2022

A.C. Amato Mangiameli (2021), *Natur@*, Giappichelli, 2021

125. L'istituto dell'art. 1374 c.c. può essere invocato in quanto la normativa primaria (Regolamento UE) rinvia espressamente alla normativa secondaria delle Autorità indipendenti e del loro Coordinatore (Delibere ACER e ARERA), come chiarito Autorità Azara 2020.

126. I 7 parametri elencati nel documento sono: System Observability, System Controllability, Active System Management, Smart Grid Planning, Transparency in Data Access and Sharing Between Relevant Stakeholders, Local Flexibility Market and Customer Inclusion, Smart Asset Management.

127. Finnis 2013.

A.C. Amato Mangiameli (2017), *Tecno-regolazione e diritto. Brevi note su limiti e differenze*, in "Il Diritto dell'informazione e dell'informatica", 2017, n. 32

M. Ambrosoli (2014), *Condizioni generali di contratto*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, agg. 2014

L. Antoniolli (2011), *Contratti del consumatore nel diritto dell'Unione europea*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, agg. 2011

A. Azara (2020), *Fonti sub-primarie e integrazione del contratto*, in "Giustizia Civile", 2020, n. 1

R. Baldwin (1995), *Rules and Government*, Clarendon Press, 1995

R. Baldwin, M. Cave (1999), *Understanding Regulation: Theory, Strategy and Practice*, Oxford University Press, 1999

L. Balestra (2023), *Proprietà e soggettività delle comunità energetiche: profili privatistici*, in "Giurisprudenza italiana", 2023, n. 12

G. Barozzi Reggiani (2020), *Il «dominio delle regole». La regolazione indipendente dei settori dell'energia elettrica e del gas naturale tra matrice europea e politica nazionale*, Giappichelli, 2020

F. Bartolini (2023), *I contratti di godimento per lo sviluppo delle comunità energetiche*, in "Giurisprudenza italiana", 2023, n. 12

A.M. Benedetti (2021), *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in "Rivista di diritto civile", 2021, n. 3

D. Bevilacqua (2024), *La dialettica tra la promozione delle energie rinnovabili e la tutela di altri beni ambientali*, in "Giornale di diritto amministrativo", 2024, n. 1

M.L. Bixio (2023), *Blockchain, tracciabilità e marchi di certificazione*, in "Il Diritto industriale", 2023, n. 2

C. Buzzacchi (a cura di) (2011), *L'Europa a rete: il modello delle reti tra concorrenza e coesione sociale*, Giuffrè, 2011

G. Calandra (1965), *Elettricità ed elettrificazione*, in "Enciclopedia del Diritto", Giuffrè, 1965

A. Candido (2011), *Verso il mercato interno dell'energia: le reti energetiche europee*, in C. Buzzacchi (a cura di), "L'Europa a rete: il modello delle reti tra concorrenza e coesione sociale", Giuffrè, 2011

A. Cataudella (2019), *I contratti*, Giappichelli, 2019

A. Cataudella (1998), *Scritti sui contratti*, Cedam, 1998

U. Cerasoli (2008), *Autorità amministrative indipendenti nel diritto europeo*, in "Digesto delle Discipline Pubblicistiche", UTET, agg. 2008

S.A. Cerrato, G. Culasso, E. Crocco (2023), *"Handle with care". Per una governance dell'intelligenza artificiale nell'impresa: rischi, tecniche di gestione, assetti cibernetici*, in "Rivista delle società", 2023, n. 2-3

S.A. Cerrato (2020), *Appunti su smart contract e diritto dei contratti*, in "Banca borsa e titoli di credito", 2020, n. 3

V. Cerulli Irelli (2022), *Proprietà, beni pubblici, beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

V. Cerulli Irelli (2016), *Beni comuni e diritti collettivi*, in "Democrazia e Società", 2016, n. 3

C. Chiariello (2017), *Ambiente (diritto all')*, in "Digesto delle Discipline Pubblicistiche", agg. VII, UTET, 2017

A. Colavecchio (2005), *Energia elettrica*, in "Digesto delle Discipline Pubblicistiche", agg. II, UTET, 2005

G.D. Comporti, S. Lucattini (2020), *Orizzonti del diritto dell'energia. Innovazione tecnologica, blockchain e fonti rinnovabili*, Editoriale Scientifica, 2020

A. Contaldo, F. Campana (2019), *Blockchain, criptovalute, smart contract, industria 4.0*, Pacini Giuridica, 2019

C. Contessa (2024), *La disciplina dei settori speciali fra novità e conferme*, in "Rivista italiana di diritto pubblico comunitario", 2024, n. 1

G. Cordini (1987), *Ambiente (tutela dell') nel diritto delle comunità europee*, in "Digesto delle Discipline Pubblicistiche", UTET, 1987

M. D'Addezio (2018), *Agroenergia (diritto dell'Unione europea e interno)*, in "Digesto delle Discipline Privatistiche", Sezione Civile, agg. XI, UTET, 2018

G. D'Amico (2023), *Il Contratto o i contratti?*, in "Rivista di diritto civile", 2023, n. 3

M. De Bellis (2006), *Energia elettrica*, in S. Cassese (a cura di), "Dizionario di Diritto Pubblico", Giuffrè, 2006

G. Del Tin (1987), *Energia*, in "Grande Dizionario Enciclopedico", vol. VII, UTET, 1987

L. Di Bona (2008), *Potere normativo delle autorità indipendenti e contratto. Modelli di eteronomia negoziale nei settori dell'energia elettrica e del gas*, Edizioni Scientifiche Italiane, 2008

L. Di Cerbo (2023), *Il nomos delle comunità energetiche: tra Stato, mercato e comune*, in "Giurisprudenza italiana", 2023, n. 12

F. Di Ciommo (2019), *Smart contract e (non-)diritto: il caso dei mercati finanziari*, in "Nuovo diritto civile", 2019, n. 1

EU Blockchain Observatory and Forum Experts Panel (2022), *Smart contracts*, EU Blockchain Observatory and Forum, 2022

European Commission, Directorate General for Communications Networks, Content and Technology (2021), *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach*, Publications Office of the European Union, 2021

European Commission, Directorate-General for Energy (2019), *Clean energy for all Europeans*, Publications Office of the European Union, 2019

C. Favilli (2023), *Transizione ecologica e autoconsumo organizzato di energia rinnovabile. La questione della forma giuridica delle comunità energetiche*, in "Responsabilità Civile e Previdenza", 2023, n. 2

R. Federici (2015), *Concetto giuridico di energia*, in E. Picozza, S.M. Sambri (a cura di), "Il diritto dell'energia", vol. X, in E. Picozza, E. Gabrielli (diretto da), "Trattato di diritto dell'economia", Cedam, 2015

R. Fercia (2013), *Contratto normativo*, in "Digesto delle Discipline Privatistiche", Sezione Civile, agg. VIII, UTET, 2013

C. Ferrari (2018), *I contratti dei mercati regolati*, Giappichelli, 2018

E. Ferrero (2020), *Le comunità energetiche: ritorno a un futuro sostenibile*, in "Ambiente e sviluppo", 2020, n. 8-9

F. Festi (2015), *Il diritto dei contratti regolati*, in Aa.Vv., "Dialoghi sul diritto dell'energia", vol. II, Contratti dell'energia e regolazione, Giappichelli, 2015

J. Finnis (2013), *Human Rights and Common Good: Collected Essays*, vol. III, Oxford University Press, 2013

G. Finocchiaro (2022), *La regolazione dell'intelligenza artificiale*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

R. Fiori (2003), *Il problema dell'oggetto del contratto nella tradizione civilistica*, in Aa.Vv., "Modelli teorici e metodologici nella storia del diritto privato", Jovene, 2003

E. Gabrielli (2012), *Il contratto e il suo oggetto nel diritto italiano*, in "Rivista trimestrale di diritto e procedura civile", 2012, n. 1

E. Gabrielli (2009), *L'operazione economica nella teoria del contratto*, in "Rivista trimestrale di diritto e procedura civile", 2009, n. 3

E. Gabrielli (2006), *Sulla nozione di consumatore*, in Aa.Vv., "Studi in onore di C.M. Bianca", tomo III, Giuffrè, 2006

E. Gabrielli (2004), *Storia e dogma dell'oggetto del contratto*, in "Rivista di diritto civile", 2004, n. 1

E. Gabrielli (2001), *L'oggetto del contratto*, in "Il codice civile. Commentario", diretto da P. Schlesinger, Giuffrè, 2001

E. Gabrielli, U. Ruffolo (a cura di) (2019), *Intelligenza artificiale e diritto*, in "Giurisprudenza italiana", 2019, n. 7

E. Gabrielli, U. Ruffolo (2019-a), *Introduzione*, in Id. (a cura di), "Intelligenza artificiale e diritto", Giurisprudenza italiana, 2019, n. 7

P. Gallo (2022), *Smart contracts e agenti software*, in "Digesto delle Discipline Privatistiche", Sezione Civile, agg., UTET, 2022

A. Gentili (2022), *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in "Rivista trimestrale di diritto e procedura civile", 2022, n. 3

M.S. Giannini (1963), *I beni pubblici: dispense delle lezioni del corso di diritto amministrativo tenute nell'anno accademico 1962-1963*, Bulzoni, 1963

L. Gili (2008), *Efficienza Energetica*, in "Digesto delle Discipline Pubblicistiche", agg. III, UTET, 2008

G. Gitti (2006), *L'autonomia privata e le Autorità indipendenti*, il Mulino, 2006

G. Gitti (2006-a), *L'oggetto del contratto e le fonti di determinazione dell'oggetto dei contratti di impresa*, in Aa.Vv., "Studi in onore di C.M. Bianca", tomo III, Giuffrè, 2006

High-Level Expert Group on Artificial Intelligence (2020), *Assessment List for Trustworthy AI (ALTAI)*, European Commission, Brussels, 2020

High-Level Expert Group on Artificial Intelligence (2019), *Policy and Investment Recommendations for trustworthy AI*, European Commission, Brussels, June 2019

High-Level Expert Group on Artificial Intelligence (AI HLEG) 2019-a, *Ethics guidelines for trustworthy AI*, European Commission, Brussels, 2019

M. Iaselli (2022), *Contratti informatici,* Pacini Giuridica, 2022

D. Imbruglia (2023), *Le presunzioni delle macchine e il consenso dell'interessato*, in "Rivista trimestrale di diritto e procedura civile", 2023, n. 3

N. Irti (2004), *L'ordine giuridico del mercato*, Laterza, 2004

A.U. Janssen, F.P. Patti (2020), *Demistificare gli smart contracts*, in "Osservatorio del Diritto Civile e Commerciale", 2020, n. 1

G. Landi (1965), *Energia elettrica (nazionalizzazione)*, in "Enciclopedia del Diritto", Giuffrè, 1965

R. Lener (2023), *Criptoattività e criptovalute alla luce degli ultimi orientamenti comunitari*, in "Giurisprudenza commerciale", 2023, n. 3

R. Lener (2022), *Cripto-attività e criptovalute alla luce degli ultimi orientamenti comunitari*, in M. Callegari, S.A. Cerrato, E.R. Desana (a cura di), "Governance e mercati. Studi in onore di Paolo Montalenti", Giappichelli, 2022

P. Lillo (2024), *Diritti fondamentali e libertà della persona*, Giappichelli, 2024

A. Lucarelli (2021), *Beni comuni*, in "Digesto delle Discipline Pubblicistiche", agg. VIII, 2021

L.M. Lucarelli Tonini (2023), *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di 'ai liability directive'*, in "Il Diritto dell'informazione e dell'informatica", 2023, n. 2

F. Macario, N. Mazzia (1991), *Energia (somministrazione di)*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1991

G. Majone (2001), *Nonmajoritarian Institutions and the Limits of Democratic Governance: A Political Transaction-Cost Approach*, in "Journal of Institutional and Theoretical Economics", 2001, n. 157

G. Marchetti (2022), *Lineamenti evolutivi della potestatività condizionale: dal contratto allo smart contract*, in "Rivista di diritto civile", 2022, n. 1

F. Marinelli (2014), *Beni comuni*, in "Enciclopedia del Diritto", ann. VII, Giuffrè, 2014

M. Marletta (2014), *Il quadro giuridico europeo sulle energie rinnovabili*, in "Diritto dell'Unione Europea", 2014, n. 3

B. Marone (2022), Legal design *e forma computazionale del contratto: questo matrimonio s'ha da fare?*, in "Contratti", 2022, n. 6

E.D. Martino, W.G. Ringe (2024), *The social cost of blockchain. Externalities, allocation of property rights and the role of law*, Hamburg ILA Working Paper Series n. 80, 2024

M. Maugeri (2021), *Smart contracts*, in "Enciclopedia del Diritto", Giuffrè, 2021

M. Maugeri (2021-a), *Smart Contracts e disciplina dei contratti*, il Mulino, 2021

M. Maugeri (2020), *Smart Contracts, smart grids e smart meters: i nuovi orizzonti nel mercato dell'energia e la tutela del consumatore/prosumer*, in G.D. Comporti, S. Lucattini (a cura di), "Orizzonti del diritto dell'energia. Innovazione tecnologica, blockchain e fonti rinnovabili", Editoriale Scientifica, 2020

F. Merusi, S. Antoniazzi (a cura di), (2017), *Vent'anni di regolazione accentrata di servizi pubblici locali*, Giappichelli, 2017

F. Merusi, M. Passaro (2002), *Autorità indipendenti*, in "Enciclopedia del Diritto", agg. VI, Giuffrè, 2002

D. Messina (2023), *La tutela della dignità nell'era digitale*, Editoriale Scientifica, 2023

D. Messinetti (1965), *Energia*, in "Enciclopedia del Diritto", Giuffrè, 1965

M.F. Monterossi (2021), *Blockchain (diritto pubblico)*, in "Digesto delle Discipline Pubblicistiche", agg. VIII, UTET, 2021

A. Morace Pinelli (a cura di) (2024), *Dalla* Data Protection *alla* Data Governance*: il Regolamento (UE) 2022/868. Commentario al* Data Governance Act, Pacini Giuridica, 2024

A. Morace Pinelli (a cura di) (2023), *La circolazione dei dati personali: persona, contratto e mercato*, Pacini Giuridica, 2023

U. Morello (1988), *Condizioni generali di contratto*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1988

R. Moro Visconti (2024), *Intelligenza artificiale e network digitali: valutazione economica e implicazioni giuridiche*, in "Il Diritto Industriale", 2024, n. 1

S. Nakamoto (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

G. Nuzzo (2022), *Impresa e società nell'era digitale (appunti)*, in "Banca borsa e titoli di credito", 2022, n. 3

M. Olivetti (2022), *Gli altri diritti fondamentali*, Giappichelli, 2022

G. Oppo (2006), *I contratti d'impresa tra codice civile e legislazione speciale*, in Aa.Vv., "Studi in onore di C.M. Bianca", tomo III, Giuffrè, 2006

E. Ostrom (1990/2006), *Governare i beni collettivi*, trad. it., Marsilio, 2006

E. Ostrom (1990), *Governing the Commons. The evolution of institutions for collective actions*, Cambridge University Press, 1990

F. Pace (2007), *Contratto di interconnessione*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, agg. 2007

G. Palermo (1991), *Il contratto preliminare*, Cedam, 1991

R. Pardolesi (1991), *Energia*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1991

L. Pergolizzi (2021), *Il processo di transizione verso la promozione dell'efficientamento energetico nell'ottica della rigenerazione urbana: il "caso" degli impianti alimentati da fonte geotermica*, in "Rivista giuridica dell'edilizia", 2021, n. 3

G. Pericu (1987), *Ambiente (tutela dell') nel diritto amministrativo*, in "Digesto delle Discipline Pubblicistiche", agg. 2011 a cura di F. Pavoni, UTET, 1987

M.L. Perugini (2018), Distributed Ledger Technologies *e sistemi di* Blockchain, Key Editore, 2018

E. Picozza, S.M. Sambri (a cura di) (2015), *Il diritto dell'energia*, vol. X, in E. Picozza, E. Gabrielli (diretto da), "Trattato di diritto dell'economia", Cedam, 2015

A. Pirozzoli (2024), *Intelligenza artificiale, sviluppo sostenibile e ambiente*, in "Consulta Online", 2024, n. 1

M. Poto (2008), *Autorità amministrative indipendenti*, in "Digesto delle Discipline Pubblicistiche", UTET, 2008

B. Pozzo (2003), *Ambiente (Strumenti privatistici di tutela dell')*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 2003

S. Preziosi (2022), *La responsabilità penale per eventi generati da sistemi di IA o da processi automatizzati*, in R. Giordano, A. Panzarola, A. Police et al. (a cura di), "Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia", Giuffrè, 2022

S. Preziosi (2008), *La manipolazione di mercato*, Cacucci, 2008

C. Prussiani (2022), *La conformazione contrattuale nei settori regolati dalle autorità amministrative indipendenti: un'ipotesi di studio*, Giuffrè, 2022

P. Ranci (2017), *L'avvio dell'autorità: una valutazione in retrospettiva*, in F. Merusi, S. Antoniazzi (a cura di), "Vent'anni di regolazione accentrata di servizi pubblici locali", Giappichelli, 2017

N. Rangone (2023), *Regolare con l'intelligenza artificiale*, in "Diritto amministrativo", 2023, n. 4

M. Renna (2024), *Le comunità energetiche e l'autoconsumo collettivo di energia. Tutela della concorrenza e regolazione del mercato*, in "Le Nuove Leggi Civili Commentate", 2024, n. 1

M. Renna (2022), *Beni pubblici*, in "Enciclopedia del Diritto", I tematici – III Funzioni Amministrative, Giuffrè, 2022

C. Romeo (2024), *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in "Il Lavoro nella giurisprudenza", 2024, n. 1

G. Salito (2019), *Smart contract*, in "Digesto delle Discipline Privatistiche", Sezione Civile, agg. XII, UTET, 2019

M.G. Salvadori (1995), *Normativo (contratto)*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1995

A.M. Sandulli (1959), *Beni pubblici*, in "Enciclopedia del Diritto", Giuffrè, 1959

G. Sartor (2022), *L'intelligenza artificiale e il diritto*, Giappichelli, 2022

C. Scognamiglio (2006), *Contratti d'impresa e volontà delle parti contraenti*, in Aa.Vv., "Studi in onore di C.M. Bianca", Giuffrè, 2006

D. Simeoli (2015), *Il contratto "regolato": spunti per uno studio*, in Aa.Vv., "Dialoghi sul diritto dell'energia", vol. II, Contratti dell'energia e regolazione, Giappichelli, 2015

D. Simeoli (2014), *Contratto e potere regolatorio*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 2014

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal – Rivista di Biodiritto", 2019, n. 1

B. Sirgiovanni (2023), *Lo 'smart contract' e la tutela del consumatore: la traduzione del linguaggio naturale in linguaggio informatico attraverso il legal design*, in "Le Nuove Leggi Civili Commentate", 2023, n. 1

B. Sirgiovanni (2022), *La tutela del cliente-consumatore nel mercato unico digitale*, in R. Giordano, A. Panzarola, A. Police et al. (a cura di), "Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia", Giuffrè, 2022

B. Sirgiovanni (2017), *Dal diritto sui beni comuni al diritto ai beni comuni*, in "Rassegna di diritto civile", 2017, n. 1

C. Solinas (2018), *Il contratto "amministrato". La conformazione dell'operazione economica privata agli interessi generali*, Edizioni Scientifiche Italiane, 2018

A. Spatuzzi (2023), *Algoritmi e automazione: la notte del contratto?*, in "Notariato", 2023, n. 3

N. Szabo (1994), *Smart contracts*, 1994

M. Thatcher, A. Stone Sweet (2002), *Theory and Practice of Delegations to Non-Majoritarian Institutions*, in "West European Politics", 2002, n. 25

O. Troiano (1991), *Energia (risparmio di)*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1991

UNESCO (2021), *Recommendation on Ethics of Artificial Intelligence*, 23 November 2021

M. Vatiero (2022), *Smart contracts vs incomplete contracts: a transaction cost economics viewpoint*, in "Computer Law and Security Review", vol. 46, 2022, n. 105710

P. Vitucci (1991), *Energia solare ed eolica*, in "Digesto delle Discipline Privatistiche", Sezione Civile, UTET, 1991

K. Werbach, N. Cornell (2017), *Contracts ex machina*, in "Duke Law Review", vol. 67, 2017, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0224 • articolo non sottoposto a peer review • pubblicato in anteprima il 26 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Elio Fameli

in collaborazione con **Enrico Bisenzi**

La nuova Intelligenza artificiale e il problema della sua regolazione giuridica. La strategia europea e il lungo iter legislativo dell'AI Act

La rivoluzione tecnologica in corso in questi ultimi anni, soprattutto nel campo dell'Intelligenza artificiale (IA) e dell'apprendimento automatico, ha aperto scenari assolutamente nuovi e, fino a pochi anni fa, del tutto inimmaginabili. Il computer non è più la macchina inerte che si limita a eseguire le istruzioni impartite dal programmatore, ma, in quanto dotato di "capacità di apprendimento", diviene interlocutore attivo, in grado non solo di registrare enormi masse di dati, ma anche di elaborarle estraendone nuova conoscenza. Di fronte a questo rapido sviluppo tecnologico, l'Ue si è trovata nella necessità di affrontare con urgenza il problema della sua disciplina giuridica. La Legge europea sulla IA (AI Act), recentemente entrata in vigore, ponendosi a conclusione di un lungo e faticoso percorso, pur con i suoi inevitabili limiti, si configura come prima esperienza di regolazione organica e strutturata dell'Intelligenza artificiale nella molteplicità delle sue applicazioni.

Intelligenza artificiale – Apprendimento automatico – Rapporto uomo-computer – Strategia europea per l'IA
AI Act – Considerazioni critiche sull'AI Act

The new Artificial Intelligence and the problem of its legal regulation. The european strategy and the long legislative process of the AI Act

The technological revolution that has taken place in recent years, especially in the field of Artificial Intelligence (AI) and machine learning, has opened up completely new scenarios that were unimaginable just a few years ago. The computer is no longer an inert machine that simply executes the instructions given by the programmer in a rigid and sequential manner but, because it is endowed with "learning capabilities", it becomes an active interlocutor, capable not only of absorbing enormous amounts of data, but also of processing them, extracting new knowledge from them. In the face of this rapid technological development, the EU was faced with the urgent need to address the problem of its legal regulation. The European AI Act comes at the end of a long and arduous journey and, despite its inevitable limitations, is the first experience of organic and structured regulation of Artificial Intelligence in the multiplicity of its applications.

Artificial Intelligence – Machine Learning – Human-computer interaction – European AI Strategy –AI Act
Critical remarks on the AI Act

La Rivista è felice di ospitare le riflessioni proposte in questo saggio da Elio Fameli, componente del consiglio scientifico della RIID, in collaborazione con Enrico Bisenzi. E. Fameli è dirigente di ricerca in quiescenza del CNR (Istituto di Informatica Giuridica e Sistemi Giudiziari - IGSG di Firenze). E. Bisenzi è docente di "Inclusive Design" (Settore: "Graphic Design") presso l'Accademia di Belle Arti di Roma. Il presente contributo è frutto della piena condivisione di idee e opinioni tra gli Autori

Sommario: 1. Introduzione: l'uomo e la macchina a confronto, tra prospettive di progressi fantascientifici e timori di scenari apocalittici. – 2. La rivoluzione dell'Intelligenza artificiale: il paradigma dei giochi strategici e il passaggio dall'approccio analitico a quello euristico nella soluzione dei problemi complessi. – 2.1. Il punto di svolta nell'evoluzione dell'Intelligenza artificiale: dalla potenza di calcolo alla capacità di apprendimento. – 2.2. L'apprendimento automatico e la pervasività delle nuove tecnologie. – 2.3. La "Teoria della mente" e la nuova configurazione del rapporto uomo-computer. – 3. Il problema della regolazione giuridica dell'Intelligenza artificiale: l'approccio europeo. – 3.1. La diffusione dell'Intelligenza artificiale: opportunità e rischi. – 3.2. Il contesto geopolitico e gli obiettivi della politica europea per l'IA. – 4. La Legge europea sull'Intelligenza artificiale (AI Act): entrata in vigore e ambito di applicazione. – 5. Considerazioni finali: ultimi sviluppi dell'Intelligenza artificiale e prime valutazioni dell'AI Act.

1. Introduzione: l'uomo e la macchina a confronto, tra prospettive di progressi fantascientifici e timori di scenari apocalittici

Dopo una fase di apparente letargo, scarsa visibilità e diffuso scetticismo, da alcuni anni l'Intelligenza artificiale (IA) sta conoscendo un periodo di rigoglioso sviluppo e sempre più vaste applicazioni, fino al punto di configurarsi come il settore di ricerca più avanzato e coinvolgente, quello – in ultima analisi – in cui si dovranno presumibilmente registrare le conquiste più affascinanti del futuro. La presenza pervasiva dell'IA è ormai una costante del nostro vivere quotidiano: tra le mura domestiche come in auto, al lavoro come nel divertimento, ci troviamo continuamente – ma spesso anche in maniera inconsapevole – a interagire con strumenti, dispositivi e, più di recente, "assistenti intelligenti". Ogni giorno, ormai senza rendercene conto, interagiamo con "macchine intelligenti" che indirizzano le nostre telefonate, approvano gli acquisti con carta di credito, interpretano gli esami medici, compongono musica e creano persino opere d'arte. Presto, inoltre, le automobili a guida autonoma percorreranno le strade di tutto il mondo. Negli anni Cinquanta del Novecento sognavamo di costruire intelligenze simili a quella dell'uomo. Oggi abbiamo creato macchine che, elaborando grandi quantità di dati, riescono a riconoscerci e a prendere decisioni. Non ci chiediamo più neppure chi ci stia educatamente rispondendo al telefono, con chi stiamo utilmente conversando sul computer, chi ci stia fornendo preziose indicazioni sul viaggio da intraprendere o lo svago da preferire. Intorno a noi si moltiplicano "soggetti" senza volto, che dimostrano però di conoscere bene il nostro "profilo", anche nei suoi aspetti più delicati e sensibili, dalla collocazione sociale al livello culturale, dalle convinzioni religiose all'orientamento politico.

Dei rischi connessi agli sviluppi e alla diffusione dell'IA si sono occupate menti eccelse e personalità illustri, nel campo della scienza, della finanza, ma anche dell'economia e della politica. Così, secondo il celebre cosmologo Stephen Hawking, l'umanità avrebbe ormai raggiunto un punto di non ritorno in quanto l'IA arriverà presto a un livello tale da superare di gran lunga la specie umana, configurandosi come una nuova forma di vita. Se, da una parte, è incontestabile che i progressi nel campo dell'IA possono portare benefici inimmaginabili alla società, è comunque altrettanto certo che risulta inevitabilmente molto sottile la linea di confine tra i vantaggi che si possono ricavare dalla tecnologia e il pericolo che questa ci sfugga di mano: "l'AI

potrebbe essere il più grande evento nella storia della nostra civiltà, oppure il peggiore"[1].

Un giorno l'intelligenza delle macchine supererà quella degli esseri umani? Siamo dunque a un passo dall'Apocalisse, circondati da supercomputer in grado di prendere il sopravvento sull'uomo? La loro crescita e il continuo incremento della loro potenza preannuncia forse l'avvento d'una nuova era, dominata da macchine capaci di svolgere compiti complessi molto meglio e più velocemente di noi? Già diversi anni or sono questi allarmanti interrogativi emergevano, ad esempio, negli scritti raccolti da Douglas Heaven, senior editor per l'IA presso la "MIT Technology Review"[2].

Elon Musk[3], insieme a un gran numero di personalità del mondo scientifico ed esperti di robotica e Intelligenza artificiale, già nel 2017, con una lettera aperta[4] indirizzata all'ONU e resa pubblica in occasione della Conferenza mondiale sull'IA (IJCAI 2017)[5], aveva lanciato un accorato allarme contro lo sviluppo e l'uso di "sistemi letali autonomi", inevitabilmente destinati a provocare il disastro totale di una terza guerra mondiale. Il documento, che vedeva per la prima volta uniti i rappresentanti delle società di AI e robotica di 26 Paesi, anche per il gran numero di firmatari evidenziava la gravità e l'urgenza della situazione. Ormai non si tratta più di uno scenario ipotetico, bensì di un problema reale e concreto, che richiede risposte rapide e adeguate: a differenza di altre potenziali manifestazioni dell'IA che appartengono ancora al mondo della fantascienza, attualmente i sistemi autonomi armati sono al primo posto nella classifica degli investimenti per lo sviluppo di nuove tecnologie.

Molto di recente, sui rischi di uno sviluppo incontrollato dell'Intelligenza artificiale si sono espressi anche i due vincitori del Premio Nobel per la Fisica, John Hopfield, fisico statunitense attivo soprattutto nel campo della biofisica e della fisica statistica, e Geoffrey Hinton, psicologo e informatico britannico naturalizzato canadese, considerato uno tra i ricercatori più influenti nello sviluppo dell'apprendimento profondo. Nella motivazione del premio è messa in evidenza la grande importanza delle ricerche svolte da questi due scienziati, che hanno utilizzato gli strumenti della Fisica per porre le basi dello sviluppo attuale dell'apprendimento automatico. La capacità d'imparare in modo autonomo, basata sulle reti neurali artificiali, sta rivoluzionando la scienza, l'ingegneria e persino la nostra vita quotidiana. Hinton, in particolare, ritiene che l'Intelligenza artificiale "avrà sull'umanità conseguenze paragonabili alla rivoluzione industriale: all'epoca le macchine ci superavano in forza fisica, ora invece sono destinate a superarci dal punto di vista intellettuale. Ci saranno effetti estremamente positivi, … ma potranno esserci anche conseguenze negative, qualora le macchine riescano a sfuggire al nostro controllo"[6].

Sul fronte opposto a quello dei "preoccupati" per il continuo potenziamento delle capacità dell'IA e per il suo inarrestabile dilagare in ogni settore dell'attività umana, non mancano studiosi e divulgatori che tendono a evidenziare i limiti e gli insuccessi di computer superpotenti o di robot umanoidi impegnati in compiti anche modesti[7]. Esistono corpose raccolte di storielle da raccontare sui fallimenti di robot pur sofisticati ed evoluti, ma sembrano comunque ingenuamente rassicuranti affermazioni categoriche come quella enunciata da Will Douglas Heaven[8] in un suo articolo sull'argomento: "Far from being a steady march to greatness, the past and present of robotics and AI are littered with examples of banal practicalities tying machines down. If you want to look at what the

1. La citazione è in Intini 2017.
2. Vedi New Scientist 2018.
3. Elon Musk, imprenditore sudafricano naturalizzato statunitense, è cofondatore di OpenAI, un laboratorio di ricerca sull'Intelligenza artificiale costituito con lo specifico obiettivo di promuovere e sviluppare una IA amichevole, in grado di contribuire al benessere dell'umanità.
4. Si veda Musk et al. 2017.
5. IJCAI-17, Melbourne, August 19-25, 2017.
6. Cfr., *inter alia*, Intini 2024; Dusi 2024; Rovelli–Ottolina 2024.
7. Si vedano, tra i molti, Zreick 2018; Fleischner 2023.
8. Will Douglas Heaven è "senior editor" per l'Intelligenza artificiale presso la "MIT Technology Review".

future of AI really holds, it's not the highlight reels that matter – it's the out-takes"[9].

In realtà non mancano fatti imbarazzanti e sicuramente negativi che, a ben guardare, piuttosto che evidenziare i limiti dell'IA e delle sue applicazioni, mostrano i rischi che derivano dall'uso distorto che se ne può fare. Esemplare, in questo senso, è stata la vicenda di Tay, il chatbot di Microsoft che aveva debuttato nel 2016 su Twitter: progettato per imparare autonomamente parole ed espressioni in linguaggio naturale dialogando direttamente con gli utenti sui social, dopo poche ore dall'attivazione aveva cominciato a scrivere commenti offensivi, sessisti e razzisti. costringendo così la Microsoft a porre fine all'esperimento nel giro di 24 ore[10].

Per concludere questi brevi cenni sui rischi connessi allo sviluppo incontrollato dell'IA e sui limiti che – almeno per ora – sembrano contrassegnarne l'evoluzione, si può qui fare riferimento all'osservazione di Mark Riedl[11], secondo cui resteranno comunque fuori dalla portata del computer i linguaggi altamente veloci e complessi, con forti riferimenti contestuali e situazionali, ma anche l'umorismo, la comicità originale e innovativa, così come, per altro verso, le decisioni imprevedibili e le idee rivoluzionarie. In questo senso l'IA, basandosi sull'accesso a immense quantità di dati esistenti che poi sintetizza ed elabora, sarebbe una "tecnologia conservatrice". Com'è stato autorevolmente affermato:"Il computer, non essendo in grado di capire cosa siano i tabù, non può infrangerli"[12].

A queste ultime considerazioni, a un livello più generale e fortemente interdisciplinare, possono infine collegarsi le teorie rassicuranti di chi riafferma l'indefettibile superiorità dell'uomo sulla macchina fondando la sua ricerca non solo sul rigore scientifico, ma anche sulla visionarietà tecnologica e sull'elaborazione filosofico-religiosa[13]. Partendo dalla constatazione della deriva materialista e riduzionista che sta portando a considerare l'uomo come una macchina, si evidenzia la necessità di una nuova scienza che includa la spiritualità e di una nuova spiritualità che, a sua volta, includa la scienza; si arriva così a proporre una rivoluzionaria, ma affascinante, teoria della realtà, in cui potrebbero trovare adeguata risposta i problemi della coscienza e del libero arbitrio[14].

2. La rivoluzione dell'Intelligenza artificiale: il paradigma dei giochi strategici e il passaggio dall'approccio analitico a quello euristico nella soluzione dei problemi complessi

La trasformazione radicale cui è andata incontro l'Intelligenza artificiale nell'ultimo ventennio è espressa in maniera emblematica nell'evoluzione subita dall'approccio informatico ai giochi strategici, in particolare il gioco degli scacchi e quello del Go.

Rievocando gli entusiasmi, ma anche le paure e le polemiche, che nel 1996 e nel 1997 accompagnarono la storica gara tra Deep Blue, il calcolatore appositamente progettato dall'IBM, e Garry Kasparov, campione mondiale di scacchi, la vittoria schiacciante sull'uomo da parte dello stesso supercomputer nella versione riveduta e aggiornata, proprio per la filosofia che l'ha resa possibile, viene a configurarsi in maniera emblematica nei confronti delle radicali trasformazioni che negli ultimi due decenni si sono verificate nel campo dell'Intelligenza artificiale[15].

9. Cfr. Douglas Heaven 2017. Nello stesso senso si veda Landgrebe–Smith 2022.
10. Si vedano, tra gli altri, Wolf–Miller–Grodzinsky 2017; Metz 2018.
11. Mark Riedl, docente di "Interactive Computing" presso il "Georgia Institute of Technology" e direttore associato del "Machine Learning Center", conduce ricerche orientate allo sviluppo di tecnologie di Intelligenza artificiale e di apprendimento automatico in grado d'interagire in modo naturale con gli utenti umani.
12. L'osservazione è di Guy Hoffman (Cornell University) ed è riportata in Baum 2023.
13. Tra le opere più recenti e autorevoli, si vedano, in particolare, Faggin 2022.
14. In questo senso Faggin 2024.
15. Sulla sfida tra il supercomputer dell'IBM e il russo Garry Kasparov, campione del mondo di scacchi per ben 15 anni (1985-2000), cfr. Hsu 2004. Alcune riflessioni sul confronto uomo-macchina sono anche in Zucconi 1997.

Ugualmente, la sfida a Go[16] tra il software AlphaGo, sviluppato dalla società DeepMind di Google, e il sudcoreano Lee SeDol, uno dei campioni mondiali di questa specialità, si è conclusa nel marzo del 2016 con una sonora sconfitta per l'uomo nei confronti della macchina: un solo match vinto dall'uomo contro quattro vinti dalla macchina. Quello che è stato definito uno degli eventi più importanti nella storia dell'Intelligenza artificiale aveva avuto un precedente, con la sconfitta del campione europeo Fan Hui nel gennaio del 2016. Nel maggio 2017, poi, si era avuta un'altra conferma delle capacità, non solo logiche ma in qualche modo anche intuitive, del supercomputer di Google, con la vittoria sul cinese Ke Jie, detentore del titolo di campione del mondo di questo millenario gioco strategico.

La complessità dei due giochi è estrema tanto che, superati certi parametri, può essere soltanto immaginata. Negli scacchi il numero delle combinazioni ammesse dei 32 pezzi sulle 64 caselle della scacchiera si calcola sia compreso fra 1043 e 1050, mentre la dimensione del c.d. "albero" delle mosse sarebbe addirittura di 10123. Nel Go, su una scacchiera (*goban*) con una griglia da 19 x 19 caselle i due avversari collocano pedine ("pietre") nere o bianche con l'obiettivo di controllare la zona più ampia della superficie di gioco, ma il numero limitato e la semplicità delle regole nascondono una quantità di combinazioni possibili largamente superiore a quella calcolata per gli scacchi[17].

Il passaggio dalla sfida tra Deep Blue e Garry Kasparov (1996-1997) a quella tra AlphaGo e Lee SeDol, Fan Hui e Ke Jie (2016-2017) può essere assunto a rappresentazione emblematica della rivoluzione in atto nel mondo dell'Intelligenza artificiale. Nel primo caso lo sforzo dei progettisti informatici si era concentrato sulla potenza di calcolo. Deep Blue, nella versione perfezionata nel 1997, non era un normale calcolatore elettronico, bensì un supercomputer ad altissimo parallelismo, con una rete di calcolo a 32 nodi, dove ogni singolo nodo utilizzava una scheda microchannel a 8 microprocessori VLSI (*Very Large Scale Integration*), per un totale di ben 256 microprocessori. Con questa struttura la macchina era in grado di calcolare, in condizioni ottimali, più di un miliardo di mosse al secondo e 60 bilioni in 3 minuti[18]. Diversamente da Deep Blue, il software utilizzato da AlphaGo per battere ripetutamente – e definitivamente – i campioni del mondo di questo difficilissimo gioco strategico è, invece, essenzialmente costituito da una combinazione tra tecniche d'apprendimento automatico (*Machine Learning*), basate sull'impiego di "reti neurali profonde", e tecniche di ricerca ad albero. A queste, però, è affiancata una fase estensiva d'apprendimento da gioco, in cui la macchina è messa in grado di memorizzare ed elaborare centinaia di migliaia di partite giocate da campioni umani o da altre macchine adeguatamente addestrate. I dati in input, prima di essere inviati alle reti neurali, nella fase di *pre-processing*, vengono analizzati in modo da individuarne le

16. Il Go è un gioco da tavolo strategico che ebbe origine in Cina, dove è giocato da almeno 2.500 anni. Divenuto rapidamente molto popolare nell'Asia orientale, dalla fine del XIX secolo ha cominciato a diffondersi anche in Occidente. Una presentazione sintetica, ma articolata di questo gioco, della sua storia e delle sue regole, ma anche della sua rilevanza nella letteratura, nella musica e nel cinema, oltre che nella matematica e nell'informatica, è in *Go (gioco)*, Voce in "Wikipedia. L'enciclopedia libera". Recentemente, della sfida a Go tra il software AlphaGo di Google e il campione sudcoreano Lee SeDol è tornata a occuparsi anche la stampa italiana. Cfr. La Repubblica (Red.) 2025.

17. Un proverbio coreano dice che nessuna partita di Go è mai stata giocata due volte, affermazione che risulta verosimile. Solo agli inizi del 2016, grazie all'impiego di software sofisticati e di un hardware particolarmente potente, siamo stati in grado di calcolare il numero di posizioni che le pedine possono assumere nel gioco. Le combinazioni ammesse sarebbero pari a 2,08 per dieci elevato alla centosettantesima: si tratta non di un numero infinito – come molti avevano sostenuto per secoli –, ma comunque di una cifra superiore al numero totale di atomi osservabili nell'universo. Il calcolo esatto delle posizioni ammesse per le pedine nel Go si deve a due informatici: John Tromp e Michal Koucký. Per considerazioni più approfondite si rimanda a *Go and Mathematics. Legal Positions*, Voce in "Wikipedia. L'enciclopedia libera".

18. Per una sintetica, ma chiara descrizione del supercomputer realizzato dall'IBM per il gioco degli scacchi si veda Glushenkov 2024.

principali caratteristiche e, in particolare, l'eventuale corrispondenza a modelli ricorrenti (*pattern*). Le reti neurali sono state inizialmente modellate sulla base del comportamento dei giocatori umani: con l'obiettivo d'imitarlo è stato utilizzato un database in cui sono stati memorizzati milioni di mosse tratte da partite storiche[19].

2.1. Il punto di svolta nell'evoluzione dell'Intelligenza artificiale: dalla potenza di calcolo alla capacità di apprendimento

Evitando in questa sede d'addentrarsi in descrizioni tecniche approfondite, importa qui rilevare come la fondamentale differenza tra l'approccio informatico impiegato dai progettisti del supercomputer IBM, da una parte, e la filosofia dei costruttori dell'algoritmo di AlphaGo, dall'altra, risieda proprio nel passaggio dal ricorso alla "forza bruta"[20] della potenza di calcolo alla (ri)scoperta del ruolo imprescindibile della "capacità d'apprendimento", basata sull'esperienza[21].

In questo senso l'importanza della vittoria del programma di Google sul campione mondiale in carica può ritenersi di portata storica, non solo con riferimento all'evoluzione delle tecniche di programmazione nel campo dell'Intelligenza artificiale, ma addirittura come pietra miliare nel processo di sviluppo scientifico e tecnologico dell'umanità. Alla precisione – ma anche alla rigidità – del calcolo logico-matematico vengono ad affiancarsi la flessibilità dell'adattamento, la prontezza della reazione, la velocità e l'efficienza dell'intuizione; in maniera fino a poco tempo fa del tutto imprevedibile e, comunque, in un contesto di allarmata attenzione, si cominciano a delineare, per il computer adeguatamente programmato e "addestrato", potenzialità che si potrebbero far rientrare in categorie concettuali quali l'istinto, l'intuizione e persino la creatività.

Nella sfida tra l'uomo e la macchina i tempi si accorciano[22], mentre la lotta diviene serrata: una ad una sembrano crollare le roccaforti degli "esseri umani", aggrappati a quelle prerogative essenziali (l'intelligenza, la volontà, il libero arbitrio, la responsabilità morale) che una riflessione filosofica millenaria ha individuato ed elaborato, ma anche costretti alla strenua difesa di una "superiorità" sempre più insidiata dagli "agenti artificiali". Alcune tra le tradizionali certezze cominciano pericolosamente a vacillare: l'immagine tranquillizzante del computer che esegue esclusivamente e fedelmente gli ordini (le istruzioni) che l'uomo (l'informatico programmatore) ad esso impartisce via via assume contorni meno netti, si affievolisce e s'incrina. All'orizzonte si affaccia – all'inizio timidamente, lontano dagli ambienti e dai modelli accademici, sovente nel chiuso dei laboratori informatici privati – il computer che "impara (da solo) dai dati" e che, sulla base dell'esperienza acquisita, "prende decisioni". Com'è evidente, si tratta di una vera e propria rivoluzione, capace d'incidere profondamente non solo nel mondo dell'informatica e delle sue sempre più vaste applicazioni, ma in generale in ogni settore della scienza e della cultura.

Questa nuova configurazione del ruolo del computer, proprio perché fuoriesce completamente dallo schema del mero esecutore di ordini, del

19. Dopo l'ultima vittoria contro il campione del mondo Ke Jie, con un comunicato stampa della DeepMind fu annunciato il ritiro di AlphaGo dalle competizioni. Gli scienziati che avevano lavorato alla sua realizzazione tennero a evidenziare che l'esperienza acquisita sarebbe stata sicuramente utilizzabile in altri settori applicativi, tra cui la "polizia predittiva" (*predictive policing*), la sanità e le energie rinnovabili. Si veda Silver–Huang–Maddison et al. 2016.

20. Il metodo "Brute Force" ("forza bruta" o "ricerca esaustiva") in Informatica è un algoritmo di risoluzione di un dato problema, che consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trovi quella effettivamente corretta.

21. Si veda in McAfee–Brynjolfsson 2016: "…So, why is AlphaGo's victory significant?…What changed? The AlphaGo victories vividly illustrate the power of a new approach in which instead of trying to program smart strategies into a computer, we instead build systems that can learn winning strategies almost entirely on their own, by seeing examples of successes and failures".

22. La vittoria di AlphaGo su Lee SeDol, il 15 marzo 2016, è arrivata improvvisa e inaspettata: qualunque esperto stimava che il dominio umano nel gioco del Go sarebbe rimasto incontrastato per un periodo di almeno 5-10 anni. Si veda Maggiolo 2016.

tutto controllabile e prevedibile, suscita immediatamente interrogativi e perplessità. Tornando all'emblematica sfida tra uomo e computer al gioco del Go, si è opportunamente messo in rilievo che la schiacciante vittoria conseguita dalla macchina sull'uomo non è stata – e non poteva essere – in alcun modo il risultato dell'analisi di tutte le combinazioni possibili nel posizionamento delle pedine. Come già precisato[23], il numero delle "posizioni ammesse" (*legal positions*) per i pezzi del gioco – numero che per secoli si era ritenuto fosse addirittura infinito – è stato calcolato solo molto di recente; si tratta, però, di un valore comunque non dominabile non solo dall'uomo, ma neppure utilizzando l'enorme potenza di calcolo dei computer oggi disponibili. Proprio per questo nessuno è in grado di spiegare come si giochi a Go ai livelli più alti: gli stessi giocatori più abili non riescono ad accedere alle conoscenze che permettono di sviluppare strategie di enorme difficoltà concettuale.

Il fenomeno è ampiamente conosciuto, perché in realtà non riguarda soltanto il gioco del Go, bensì molti tra i problemi che ci si trova quotidianamente ad affrontare nella vita quotidiana, dalla guida di un veicolo, in cui è necessario porre in essere sequenze di movimenti rapidi e coordinati, al riconoscimento di caratteri e di volti all'interno d'insiemi costituiti da migliaia di altri elementi simili. Come lo scienziato e filosofo ungherese Michael Polanyi[24] aveva efficacemente espresso, "sappiamo più cose di quelle che riusciamo a spiegare": la vera conoscenza, dunque, non può essere integralmente formalizzata in regole o algoritmi, essendo soprattutto "conoscenza tacita". Questa osservazione assume un'importanza cruciale nel dibattito sulla possibilità di costruire "macchine intelligenti", in grado di risolvere problemi complessi, dal momento che consente di prescindere dalla necessità di possedere una conoscenza analitica, esplicita e organizzata della materia da trattare. Il celebre paradosso espresso nel dialogo platonico *Menone*, in cui Socrate stesso argomenta che all'uomo non è possibile né cercare quello che sa (in quanto da lui già conosciuto), né cercare quello che non sa (perché non saprebbe cosa cercare), attraverso la rivisitazione speculativa di Polanyi, torna ad essere incredibilmente attuale. Di fronte a problemi con un grado di complessità molto elevato l'uomo è in grado di trovare soluzioni sulla base di conoscenze che egli stesso non è in grado di spiegare.

Per la realizzazione di un software in grado d'affrontare problemi di elevata complessità è necessario abbandonare la strada della previsione analitica di tutte le strategie alternative, affidando invece direttamente alla macchina il compito d'individuare le soluzioni volta a volta adeguate rispetto sia al contesto complessivo che alla sequenza delle singole situazioni critiche da superare. In questo nuovo tipo d'approccio la conoscenza che il sistema utilizza è basata sull'esperienza e, quindi, sulla valutazione di un numero altissimo d'esempi, sia di successi sia di fallimenti.

L'esplosione combinatoria – presente nel gioco degli scacchi, ma in misura molto superiore in quello del Go, come anche in quasi tutte le situazioni della vita reale in cui si ponga la necessità d'assumere decisioni in tempi ragionevoli – non consente d'avventurarsi nell'analisi d'un numero imprecisabile di possibili opzioni. L'impossibilità di prevedere e calcolare la successione e le modalità nei cambiamenti di stato rispetto alla situazione di partenza impone d'abbandonare la strada del calcolo come strumento necessario a valutare miliardi di combinazioni: anche nella pratica, di fronte a un problema da risolvere, non si esaminano tutte le possibili alternative e tutte le conseguenze di ciascuna alternativa (fatta eccezione per le ipotesi in cui esse siano poche o siano comunque riconducibili a un numero limitato). Quando la situazione è complessa si rende necessario restringere lo spazio virtuale in cui effettuare la ricerca della soluzione del problema e quindi "potare" l'albero dei percorsi astrattamente possibili per ottenere il risultato desiderato. Diventa possibile gestire l'esplosione

23. Si vedano le indicazioni fornite nella nota n. 16.

24. Michael Polanyi è stato uno dei maggiori esponenti della "nuova filosofia della scienza" nella seconda metà del ventesimo secolo. Insieme a Thomas Khun, in aperta polemica con Karl Popper, fu protagonista di quella stagione cruciale del pensiero filosofico che portò a una profonda revisione e, quindi, al rinnovamento del modo d'intendere e valutare la ricerca scientifica. Il concetto di "conoscenza inespressa" o "conoscenza tacita" (*tacit knowledge*) è sviluppato nelle opere più note di questo autore, peraltro ancora poco conosciuto e studiato. Si vedano: Polanyi 1958; Polanyi 1966.

combinatoria solo avvalendosi di una "euristica" che consenta di scartare rapidamente alcune tra le opzioni teoricamente configurabili in modo da concentrare l'attenzione su un numero limitato di alternative rimaste.

2.2. L'apprendimento automatico e la pervasività delle nuove tecnologie

In via preliminare occorre, intanto, prendere coscienza del fatto che anche l'utente medio del computer ottiene informazioni e utilizza servizi che sono comunque il risultato di forme più o meno complesse di "apprendimento automatico" da parte della macchina. Quando si effettua una ricerca nella Rete, i dati che si ottengono in risposta – come anche gli annunci pubblicitari che ne rendono più lenta e faticosa la lettura – sono stati previamente selezionati e organizzati da complessi algoritmi di *machine learning*. L'utilizzo dei servizi di *social networking*, ormai sempre più diffuso e coinvolgente soprattutto su piattaforme come Facebook e X, ma anche le varie possibilità d'acquisto e vendita di beni e servizi nel Web si avvalgono ampiamente delle tecniche di autoapprendimento. Ugualmente avviene per la segnalazione di un libro come per l'offerta di un "pacchetto vacanze", per le proposte di brani musicali o la scelta di eventi d'intrattenimento, tutte in qualche modo "calibrate" sulle preferenze dell'utente.

La presenza attiva del *machine learning*, tuttavia, non è limitata al cyberspazio: nell'arco della giornata ci accompagna, invisibile e discreta, ottimizzando i consumi del veicolo che guidiamo, controllando e adattando in continuazione la temperatura degli ambienti in cui viviamo, agevolando e supportando il lavoro d'ufficio con "software intelligenti", in grado di selezionare e organizzare la posta elettronica, estrarre le informazioni rilevanti da grandi masse di dati, effettuare traduzioni e controllare la correttezza ortografica e grammaticale dei testi. Con l'aiuto di "sistemi di apprendimento automatico" possono essere gestiti i nostri risparmi dalle banche, può essere approvata la richiesta di un mutuo, può essere controllato l'uso di una carta di credito, eseguita l'analisi dei test per l'ammissione a un corso di studi, effettuata la valutazione dell'immobile che si vuole vendere o comprare, persino decisa la dislocazione delle pattuglie di polizia nelle aree urbane a maggior rischio di criminalità. Tutto questo, e molto altro ancora, nel mondo che ci circonda come all'interno della nostra sfera privata, già oggi, sovente a nostra insaputa, costituisce il risultato delle complesse elaborazioni svolte dagli "algoritmi di apprendimento".

Una rivoluzione profonda sta trasformando la nostra vita, a livello sia individuale che sociale, ma anche la scienza, la tecnologia, l'economia, la finanza, la politica e la guerra stessa. Il *machine learning* viene a configurarsi come l'unico strumento potenzialmente in grado di gestire e convertire in conoscenza le enormi masse di dati che ci vengono fornite dalle moderne forme d'indagine della natura e dell'uomo. Tra queste ci si limita qui a citare i satelliti artificiali[25], gli acceleratori di particelle[26] e i sequenziatori di DNA[27].

L'economia, la finanza, il mondo degli affari si avvalgono ampiamente del *machine learning*. Mai prima d'ora era stato possibile ottenere una

25. Con il termine "satellite artificiale" ci si riferisce a tutti gli oggetti orbitanti intorno a un corpo celeste, posti volutamente nell'orbita desiderata con mezzi tecnologici, con varie finalità di servizio, d'indagine o di monitoraggio scientifico-ambientale. L'insieme di più satelliti artificiali adibiti a uno stesso scopo forma una "costellazione" o "flotta". Da quando, nel 1957, l'allora Unione Sovietica lanciò lo Sputnik 1, si calcola che siano stati messi in orbita intorno alla Terra oltre 14.000 satelliti artificiali; di questi, però, oltre il 75% non sarebbe più in funzione, affollando pericolosamente lo spazio intorno al nostro pianeta.
26. Gli acceleratori di particelle sono macchine tecnologicamente complesse che accelerano particelle microscopiche tramite l'interazione della carica elettrica con campi elettromagnetici statici e dinamici; è la realizzazione tecnica di questa interazione che differenzia i vari tipi di acceleratori. Le applicazioni sono divenute sempre più numerose: all'inizio gli acceleratori sono stati sviluppati essenzialmente per studiare gli elementi costituenti della materia e le leggi che regolano la loro interazione; in seguito, in particolare i collisori particella-antiparticella si sono rivelati utili sia per applicazioni tecnologiche che per applicazioni mediche.
27. Il genoma umano comprende centinaia di milioni di frammenti di codice genetico. Una mole di dati enorme, impossibile da analizzare in tempi brevi con l'ausilio della sola mente umana. Il sequenziamento del DNA consente ai ricercatori di decodificare tutti questi elementi, aiutandoli a svelare eventuali informazioni genetiche

conoscenza tanto approfondita, dinamica e continuamente aggiornabile, dei clienti, dei loro orientamenti nei consumi, dei loro gusti e, più in generale, delle loro stesse abitudini di vita. Nei negozi delle grandi catene di distribuzione gli approvvigionamenti delle merci e la loro stessa disposizione negli scaffali per la vendita avvengono sulla base di "modelli" che, a loro volta, governano "algoritmi di apprendimento". Così pure accade in un altro importante settore economico, quello della scelta dei libri verso cui far convergere gli acquisti dei lettori, all'interno di quel fenomeno sempre più vasto e coinvolgente che è il commercio elettronico.

Nel campo della finanza può essere qui sufficiente richiamare l'evidente incidenza che in essa hanno – a livello sia nazionale che transnazionale – i modelli per la scelta dei titoli azionari da vendere e/o acquistare. La maggior parte dei fondi d'investimento sceglie i titoli su cui investire avvalendosi di algoritmi di apprendimento, ma non mancano neppure attività interamente gestite da sistemi di apprendimento automatico. Si può ragionevolmente presumere che – in un contesto in cui i mercati finanziari non sono più luoghi fisici, ma piattaforme informatiche ("sedi di negoziazione") dove s'incrociano le proposte di acquisto e di vendita – i modelli per la selezione degli strumenti finanziari in realtà governino l'andamento della finanza mondiale in maniera meno trasparente, ma sicuramente più incisiva di qualunque autorità formalmente preposta alla regolazione e al controllo del settore.

Nei rapporti delle banche con i loro clienti l'impiego degli algoritmi di apprendimento assume sovente un ruolo determinante. Sofisticati programmi d'Intelligenza artificiale – solitamente sviluppati con caratteristiche funzionali e secondo parametri quasi del tutto privi di trasparenza per l'utenza – sovrintendono a numerose procedure operative: dall'apertura del conto corrente all'esame dei requisiti per il rilascio della carta di credito, dal controllo delle eventuali transazioni sospette alla valutazione delle richieste di prestiti e mutui, fino alla rilevazione e all'analisi della c.d. *customer satisfaction*, in cui le aspettative dell'utenza rispetto a una determinata tipologia di prodotto o servizio sono messe a confronto con le percezioni/valutazioni delle corrispondenti esperienze di uso o consumo.

Ugualmente, nell'ambito della tutela dell'ordine pubblico e della sicurezza dei cittadini ci si avvale in vario modo del *machine learning*. Per esempio: sulla base del controllo delle immagini registrate dalle telecamere di sorveglianza possono essere segnalate attività sospette alla centrale di coordinamento; sofisticati algoritmi di previsione statistica sono in grado di suggerire agli organi di polizia la più efficiente dislocazione delle pattuglie di ronda; complessi software d'identificazione biometrica consentono di raccogliere dati personali confrontandoli in tempi rapidissimi all'interno di vasti archivi specialistici. Nella lotta al crimine già si configurano scenari fantascientifici in cui unità di pubblica sicurezza formate da automobili senza guidatore pattuglieranno le strade delle metropoli in stretto contatto con le centrali operative, in modo da innalzare il livello d'efficienza nella ricerca e nella segnalazione di persone, cose o situazioni sospette.

In generale, poi, nella vita quotidiana ci si avvale continuamente – e talora anche inconsapevolmente – di strumenti tecnologici e dispositivi elettronici (computer, tablet, smartphone) fortemente caratterizzati, nello svolgimento stesso delle loro funzioni, dal ricorso a meccanismi di autoapprendimento. Veicoli senza conducente attraversano ormai in gran numero la terra, il mare e il cielo, pilotandosi da soli, né appartengono più alla fantascienza i progetti per la realizzazione di robot-postino, robot per lo svolgimento di lavori domestici[28], robot umanoidi[29] o droni per la consegna a domicilio di libri o alimenti. I nostri cellulari,

nascoste. In questo modo è possibile accedere a informazioni che riguardano il funzionamento del corpo umano, la crescita, l'invecchiamento e anche l'insorgere di malattie.

28. I robot domestici (*home robot*), ormai sempre più sofisticati e versatili, sono in grado non solo di cucinare e pulire, ma anche di sorvegliare la casa e controllare gli animali domestici. Anche in Europa progetti di robot umanoidi, in grado d'assistere gli anziani e le persone con ridotte capacità motorie, coinvolgono già da alcuni anni aziende leader e laboratori di ricerca impegnati nel campo dell'Intelligenza artificiale.

29. La "robotica umanoide", orientata alla costruzione di "macchine intelligenti antropomorfe" in grado d'interagire con l'uomo e adattarsi all'ambiente circostante, è ormai definitivamente uscita dalla fantascienza per diventare

compagni ormai inseparabili di lavoro, di viaggio e di svago, sono molto più che semplici strumenti di comunicazione: trasmettono, ricevono e organizzano – anche autonomamente – documenti e immagini, correggono gli errori di battitura, suggeriscono e completano le parole che inseriamo nei nostri testi, interpretano i comandi vocali con cui possiamo formulare richieste al nostro "Personal Assistant". Agli Assistenti Personali[30] installati sugli smartphone è posibile rivolgersi, in lingua naturale, per ottenere rapidamente informazioni che spaziano dalle previsioni meteorologiche alla ricerca di luoghi d'interesse, dalle indicazioni stradali e geografiche alle classifiche sportive, dalla descrizione di luoghi e persone alla predisposizione di promemoria e alla effettuazione di calcoli matematici e conversioni valutarie.

In ultima analisi, però, se, da una parte, si ottengono dal computer le risposte desiderate in corrispondenza alle domande che a esso sono state rivolte, dall'altra, il software impiegato acquisisce gradatamente una conoscenza sempre più precisa e circostanziata di chi lo utilizza in maniera regolare e continuativa, dei suoi dati personali, delle sue capacità lavorative e competenze professionali, ma anche delle sue abitudini di vita, delle sue relazioni sociali, come pure dei suoi gusti e orientamenti di consumo. Di tutta questa enorme massa di dati, di questa scia invisibile che ogni utente del Web, più o meno inconsapevolmente, lascia dietro di sé dopo ogni consultazione, si alimentano motori di ricerca sempre più potenti e sofisticati. Ogni interazione col computer (nelle sue varie declinazioni più recenti, che attualmente possono estendersi dal grosso server dislocato a migliaia di chilometri di distanza al piccolo smartphone d'uso quotidiano) in effetti avviene su due livelli distinti e in due direzioni opposte: nell'immediato l'utente consegue il risultato cui tende, sia esso la risposta a una domanda, la vendita o l'acquisto di un prodotto, l'esito di una transazione commerciale o di un'operazione finanziaria; sotto un diverso profilo, però, è invece il computer a ottenere qualcosa dall'utente, acquisendo i suoi dati personali, insieme a una serie d'informazioni precise e in vario modo articolate sulla sua vita e i suoi interessi.

Occorre, inoltre, osservare che, tralasciando i dati che vengono comunicati al computer in maniera trasparente e consapevole (quali i dati identificativi, anagrafici, telefonici, sanitari, gli indirizzi e-mail e i vari account richiesti dai motori di ricerca e dai servizi di *social networking*), molte altre informazioni sull'utente sono acquisite in forme sovente occulte e insidiose: per esempio, attraverso testi, documenti, registrazioni di percorsi di ricerca sulla Rete, rilevamenti effettuati dai microprocessori degli autoveicoli e dai sistemi di geolocalizzazione dei cellulari, immagini e sequenze riprese da telecamere di sorveglianza. Una così grande quantità e varietà di dati, poi, non rimane inerte e inutilizzabile, dal momento che sono

un campo di ricerca emergente, destinato ad attirare sempre più l'attenzione di ricercatori e case costruttrici. Robot simili all'uomo – dotati di braccia, gambe, sensori tattili e visivi – erano stati preconizzati dal drammaturgo ceco Karel Čapek, che per primo usò questo termine nel suo dramma dal titolo *R.U.R. Rossumovi univerzálni roboti* ("I robot universali di Rossum"), pubblicato nel 1920. Nei prossimi decenni questi androidi programmabili potranno diventare nostri compagni affidabili e servizievoli, svolgendo compiti ripetitivi, sgradevoli o altamente rischiosi. Già oggi, comunque, le realizzazioni sono numerose e interessanti, spaziando in settori applicativi diversi, dalla medicina all'assistenza agli anziani, dall'intrattenimento alle operazioni di soccorso in zone di guerra o colpite da calamità naturali. Robot umanoidi sono stati costruiti soprattutto in Giappone e in Corea, ma sperimentazioni rilevanti sono in corso anche in Europa. R1 è il nome del robot progettato e realizzato in Italia dall'Istituto Italiano di Tecnologia (IIT) di Genova; le sue capacità d'apprendimento automatico lo rendono adatto a svolgere compiti di accoglienza, assistenza e sorveglianza, non solo in ambito domestico, ma anche in alberghi, centri commerciali, stazioni ferroviarie, aeroporti, ospedali, case di riposo e luoghi di lavoro.

30. Tra i principali "assistenti personali" (*personal* - o *digital* o *smart* o *virtual* - *assistants*) installabili su dispositivi mobili, attualmente si possono citare: ClickUp, Socratic, Amazon Alexa, Cortana, Wally, Tabnine, Parrot IA, S Voice, Siri, Google Assistant. Per una sintetica presentazione delle funzioni e delle potenzialità di questi strumenti, ma anche dei rischi connessi al loro uso, si veda, oltre a *Assistente virtuale*, Voce in "Wikipedia. L'enciclopedia libera", Mialich 2021. In merito al problema dei rapporti tra assistenti digitali e tutela dei dati personali si veda Garante per la Protezione dei Dati Personali 2021.

concretamente disponibili numerosi strumenti atti a gestirli, accorparli e organizzarli.

2.3. La "Teoria della mente" e la nuova configurazione del rapporto uomo-computer

In base alle osservazioni svolte è chiaro che l'interazione col computer, come risultato del flusso d'informazioni che a esso vengono trasferite – volontariamente o involontariamente, consapevolmente o inconsapevolmente –, induce comunque la costruzione d'un vero e proprio "specchio digitale" dell'utente, considerato come mera entità di provenienza. A sua volta, poi, questo modello che viene generato, rimanendo continuamente aggiornabile, modificabile e incrementabile, diviene in qualche modo la base dei futuri "comportamenti" del computer nei confronti dell'utente stesso. Come nelle relazioni interpersonali, azioni e reazioni sono governate dai "modelli mentali" autonomamente e reciprocamente sviluppati dalle parti, allo stesso modo l'utente deve prendere coscienza del fatto che, nell'interazione col computer, gradatamente egli costruisce, in esso, un'immagine di sé; sulla base di questa, poi, gli algoritmi d'apprendimento di cui il dispositivo elettronico è dotato svilupperanno "comportamenti" ritenuti adeguati, in quanto, appunto, corrispondenti al modello che al suo interno si è venuto configurando.

A una comprensione più approfondita di questo tema – d'importanza centrale sotto molti e diversi profili, da quello economico e commerciale (basti pensare all'elaborazione delle strategie produttive, all'impostazione delle campagne pubblicitarie e, quindi, all'orientamento dei consumi) fino a quello psicologico, sociologico e giuridico (sono particolarmente rilevanti in questo ambito i fenomeni connessi allo sviluppo esponenziale del social network, ma anche le grandi trasformazioni in atto nelle scienze sociali e, in particolare, nel diritto) – giova il riferimento a quella che gli psicologi chiamano "Teoria della mente"[31].

L'espressione "Teoria della mente" (ToMM – *Theory of Mind Mechanisms*) è utilizzata sovente con significati diversi: a livello astratto, nell'ambito della "filosofia della mente", essa individua un modello ontologico e strutturale dei processi mentali, facendo esplicitamente riferimento agli studi sulla "natura della mente". All'interno della "psicologia cognitiva", invece, con questa stessa espressione si designano le analisi volte a configurare modelli del "funzionamento della mente".

Evitando di addentrarsi in indagini complesse ed estese, in cui sono coinvolte numerose discipline tra loro distinte e a volte lontane (non solo la filosofia, la psicologia, la psicoterapia, la pedagogia e la psicanalisi, ma anche la neurologia e le scienze cognitive in generale), in questa sede può ritenersi sufficiente assumere il significato e la funzione della "Teoria della mente" restringendoli e focalizzandoli su due concetti fondamentali: la "mentalizzazione" e la "metacognizione". La "mentalizzazione" è la facoltà che ci consente di rappresentare (e rappresentarci), di "tenere a mente" gli stati d'animo, i pensieri, riferibili agli altri e a noi stessi. Più ampia è, invece, l'estensione semantica del termine "metacognizione", che designa la capacità – molto probabilmente esclusiva degli esseri umani – di cercare di comprendersi in termini di stati mentali (quindi, non solo pensieri, ma anche sentimenti, desideri, credenze), in modo da poter attribuire significato all'esperienza e, quindi, riuscire in qualche modo a configurare in anticipo le reciproche azioni, sulla base della previsione dei comportamenti.

Nell'analisi dei rapporti uomo-computer, prendendo atto della rivoluzione tecnologica in corso in questi ultimi anni, soprattutto nel campo dell'Intelligenza artificiale e dell'apprendimento automatico, a questo punto si aprono scenari assolutamente nuovi e in gran parte imprevedibili: il computer non è più la macchina inerte che si limita a eseguire, in modo rigido e sequenziale, gli ordini impartitigli dal programmatore; essendo dotato di "capacità di apprendimento", esso diviene interlocutore attivo e, per certi versi, imprevedibile, in grado non solo di registrare enormi masse di dati, ma anche di elaborarle in modo da estrarne nuova conoscenza (*data mining*) e, quindi, di acquisire esperienza, sulla cui base formulare proposte d'azione o prendere decisioni.

I suggerimenti che il computer fornisce all'utente in ordine all'acquisto di beni e servizi online

31. Sulla "Teoria della mente" esiste ormai una imponente letteratura. Oltre a *Teoria della mente*, Voce in "Wikipedia. L'enciclopedia libera", tra le opere più recenti e complete ci si limita qui a segnalare: Camaioni 2016; Lecce–Cavallini–Pagnin 2010.

(il libro, il film, il brano musicale, l'albergo o l'agenzia immobiliare da selezionare) non sono esplicitamente predisposti per lo specifico utente che volta a volta effettua la consultazione, né sono stati elaborati in anticipo, in relazione a categorizzazioni teoriche più o meno ampie e comprensive. L'assoluta novità introdotta dalla tecnologia del *machine learning* è rappresentata proprio dalla caratteristica intrinseca degli algoritmi di apprendimento, in quanto capaci di sostituire alla necessità dell'analisi minuziosa di quantità indefinite di dati la possibilità di estrarre conoscenza ed elaborare esperienza sulla base di un numero ristretto di precedenti casi concreti[32].

3. Il problema della regolazione giuridica dell'Intelligenza artificiale: l'approccio europeo

L'approccio europeo all'Intelligenza artificiale fin dall'inizio è stato concepito partendo dalla considerazione dell'importanza centrale dell'IA nello sviluppo complessivo della società e nella configurazione delle modalità e dello stile di vita dell'uomo[33]. Si è efficacemente affermato che il modo in cui si affronteranno l'introduzione, l'applicazione e la diffusione di queste nuove tecnologie non semplicemente condizionerà, ma addirittura "disegnerà" il mondo del futuro. La strategia europea per l'Intelligenza artificiale si è posta, dunque, come obiettivo la trasformazione dell'Europa in un centro di riferimento a livello mondiale, non solo per la progettazione e lo sviluppo di soluzioni innovative, ma anche per la loro progressiva sperimentazione e adozione, tanto nel settore pubblico quanto in quello privato.

In ordine al conseguimento di questo risultato, già nella sua Comunicazione sul tema "Intelligenza artificiale per l'Europa"[34] la Commissione europea aveva evidenziato la necessità di: a) aumentare la capacità tecnologica e industriale dei diversi Stati dell'Unione incrementando la ricerca e l'innovazione, oltre che migliorando l'accesso ai dati; b) prepararsi ai cambiamenti socio-economici che ne deriveranno, incoraggiando la modernizzazione dei sistemi d'istruzione e formazione; c) anticipare e sostenere le transizioni e i cambiamenti nel mercato del lavoro adattando i sistemi di protezione sociale; d) infine, garantire un quadro etico e giuridico adeguato, basato sui princìpi e i valori propri dell'Unione e, quindi, in linea con la sua Carta dei diritti fondamentali[35].

Di fronte al rapido sviluppo tecnologico cui si sta assistendo negli anni più recenti, all'interno di un contesto politico internazionale in cui un numero sempre crescente di Stati investe massicciamente nell'Intelligenza artificiale, l'Unione europea si è trovata nella necessità di affrontare con urgenza il problema della sua credibilità e competitività, avendo riguardo a un ampio orizzonte temporale, in relazione, da una parte, alla molteplicità e rilevanza delle iniziative prese in questo campo soprattutto dalle grandi potenze mondiali (in particolare: Stati Uniti, Cina, Giappone e Canada), dall'altra, al

32. In questa direzione l'obiettivo che ci si pone è quello d'imparare da un solo esempio o da pochi esempi. OpenAi, l'organizzazione non-profit fondata da Elon Musk, ha diffuso un sistema di IA che consente a un robot di apprendere come svolgere un determinato compito semplicemente osservando un essere umano intento a farlo per una sola volta. Com'è facile intuire, si tratta di un progresso notevole, per quanto ancora siano necessari ulteriori affinamenti per arrivare a costruire macchine in grado di eseguire incarichi sempre più complessi senza la necessità di lunghi periodi di addestramento. L'apprendimento per imitazione è stato solitamente applicato per risolvere differenti compiti presi singolarmente. Di solito questo richiede un attento lavoro ingegneristico o un significativo numero di esempi; idealmente, invece, i robot dovrebbero essere capaci d'imparare da poche dimostrazioni, applicando poi il principio generale a nuove situazioni dello stesso tipo, senza che si richieda un lavoro ulteriore.

33. Si veda Commissione europea, *Approccio europeo all'Intelligenza artificiale*.

34. Si veda Comunicazione della Commissione, COM (2018) 237, *Intelligenza artificiale per l'Europa*, 25 aprile 2018.

35. La Carta dei diritti fondamentali dell'Unione Europea (216/C 202/02), conosciuta in Italia anche come "Carta di Nizza", è stata pubblicata nella Gazzetta ufficiale dell'Unione europea il 7 giugno 2016. Proclamata ufficialmente a Nizza nel dicembre del 2000 dal Parlamento europeo, dal Consiglio dell'Unione europea e dalla Commissione, è diventata poi giuridicamente vincolante con l'entrata in vigore del Trattato di Lisbona, nel dicembre del 2009; attualmente essa ha lo stesso effetto giuridico dei Trattati dell'Unione.

continuo e rapido sviluppo della ricerca pubblica e privata in un settore d'importanza strategica centrale. È divenuta, quindi, una priorità assoluta per l'Ue preservare e incrementare le proprie risorse in modo da poter creare un ambiente atto a stimolare gli investimenti, utilizzando anche i finanziamenti pubblici per incentivare gli investimenti privati. A questo primo obiettivo si affianca, però, l'esigenza di analizzare e affrontare i molteplici rischi che dalla sempre più vasta diffusione di queste tecnologie derivano per la tutela della salute e della sicurezza, oltre che per la garanzia dei diritti fondamentali dei cittadini.

In entrambe queste due direzioni, nel 2021 la Commissione europea si è mossa formulando una "Proposta per un quadro normativo sull'Intelligenza artificiale"[36] e un "Piano coordinato sulla revisione dell'Intelligenza artificiale"[37], essenzialmente basato su una forte collaborazione tra gli Stati membri, invitati a sviluppare e aggiornare le loro strategie nazionali in ordine alla realizzazione di una leadership globale dell'Europa in questo importante settore. Nel corso del mese di giugno 2023 il Parlamento europeo ha fissato la propria posizione negoziale in merito alla normativa sull'IA (AI Act), come primo tentativo al mondo di elaborare e strutturare un insieme di regole volte a disciplinare lo sviluppo e l'applicazione di queste nuove tecnologie. Da ultimo, poi, nel gennaio del 2024 la Commissione ha pubblicato una "Comunicazione in materia di promozione delle start-up e dell'innovazione in una IA affidabile"[38] in cui, rifacendosi ai Piani d'azione coordinati del 2018 e del 2021, definisce un quadro strategico d'investimenti per un'Intelligenza artificiale affidabile affinché l'Unione possa capitalizzare le sue risorse, in particolare la sua infrastruttura di supercalcolo, leader a livello mondiale, e promuovere un ecosistema europeo innovativo in cui le start-up e gli innovatori possano collaborare a stretto contatto con gli utilizzatori industriali e attrarre investimenti.

In merito è importante rilevare che, nella citata Comunicazione, la Commissione mostra un sostanziale cambiamento di politica nei confronti dell'IA generativa, adeguandosi ai più recenti sviluppi della tecnologia. Di conseguenza, la Legge europea sull'Intelligenza artificiale (AI Act)[39], entrata in vigore il 1° agosto 2024, include anche disposizioni sull'IA generativa, ampliando la Proposta originaria presentata dalla Commissione nell'aprile del 2021.

Lo sviluppo e l'impiego sempre più esteso dell'IA possono rappresentare un elemento di mutazione radicale nella qualità della vita, a livello sia individuale che sociale, in positivo, ma anche in negativo. È dunque evidente che la prosperità e la crescita economica dell'Europa dipenderanno strettamente dal modo in cui saranno utilizzati i dati e le tecnologie della connessione. Finora, però, secondo quanto evidenziato in una recente nota della Corte dei conti europea[40], l'Ue ha mostrato di conseguire scarsi risultati nello sviluppare un ecosistema di Intelligenza artificiale europeo; in particolare, non è riuscita a far accelerare gli investimenti nel settore a un ritmo paragonabile a quello dei *competitors* mondiali. Fin dal 2018 la Commissione europea si è impegnata in numerose iniziative, affrontando anche questioni di fondo, quali la regolazione, le infrastrutture, la ricerca e gli investimenti. Tuttavia, le misure prese non sono state adeguatamente coordinate con quelle degli Stati membri; in particolare, non è stato condotto in maniera sistematica il monitoraggio degli investimenti. Per il futuro è, dunque, da considerare imprescindibile il ricorso a

36. Vedi Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (Legge sull'Intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206, 21 aprile 2021.

37. Vedi Commissione europea 2021. Il Piano coordinato, inizialmente pubblicato nel 2018, è stato poi aggiornato nel 2021, mentre è del 2024 la comunicazione della Commissione in materia di promozione delle start-up e innovazione nell'IA affidabile, di cui alla nota successiva.

38. DOC. COM(2024)28, 24 gennaio 2024.

39. L'AI Act stabilisce regole specifiche per i modelli di AI per finalità generali (Capo V), ponendo obblighi più stringenti per le ipotesi in cui si tratti di modelli classificati come "con rischio sistemico" (art. 5 e ss.); tali norme entreranno in vigore nell'agosto del 2025.

40. Si veda la nota rilasciata dalla Corte dei conti europea 2024. Cfr. anche Pedrazzoli 2024.

una governance più forte e a investimenti pubblici e privati più mirati e consistenti.

A livello globale, nella corsa agli investimenti nell'IA, l'Unione sta incontrando numerosi ostacoli. Dal 2015 gli investimenti effettuati in strumenti di capitale di rischio sono stati molto inferiori a quelli degli Stati Uniti e della Cina; si stima che il divario tra gli Stati Uniti e l'Ue in termini di investimenti complessivi nell'IA sia più che raddoppiato tra il 2018 e il 2020. In tale contesto l'Ue ha progressivamente adottato misure atte a sviluppare al proprio interno un quadro di coordinamento orientato verso l'incremento degli investimenti e l'elaborazione di un'adeguata normativa. Come si è osservato, però, i piani predisposti dalla Commissione per l'IA nel 2018 e nel 2021, pur essendo esaustivi e ampiamente in linea con le migliori pratiche internazionali, hanno registrato forti ritardi nell'attuazione, mentre gli obiettivi d'investimento dell'Ue risultano ormai troppo vaghi e obsoleti, non essendo stati più aggiornati dal 2018. La Commissione è riuscita ad aumentare la spesa a carico del bilancio dell'Ue per progetti di ricerca nel settore dell'IA, ma non ha potenziato significativamente il cofinanziamento privato e non si è impegnata a sufficienza per garantire che i progetti di ricerca finanziati siano poi adeguatamene commercializzati e sfruttati.

3.1. La diffusione dell'Intelligenza artificiale: opportunità e rischi

Gli scenari che si aprono in conseguenza dell'introduzione sempre più estesa dell'IA nelle strutture sociali come nella vita privata dei cittadini sono estremamente vari e complessi. Se da un lato, infatti, risulta fin d'ora evidente che l'Intelligenza artificiale può rendere disponibili veicoli e mezzi di trasporto più sicuri, contribuire a migliorare la sanità, l'istruzione e la formazione, aumentare la sicurezza nello svolgimento di attività lavorative pericolose, rendere più agevole l'accesso all'informazione e, in generale, consentire lo sviluppo di nuovi servizi per i cittadini, sotto un diverso profilo è però chiaro che si sono aperte prospettive ampiamente inesplorate anche per quanto attiene al mondo delle imprese e della produzione: sarà infatti possibile sviluppare una nuova generazione di prodotti e servizi anche in quei settori in cui le aziende europee sono già presenti in una posizione di forza (come l'economia circolare[41], l'agricoltura, la sanità, la moda, il turismo), ma anche rendere più sicura la manutenzione dei macchinari, ottenere risparmi di energia, aumentare sia la produzione che la qualità, ottenere percorsi di vendita più fluidi ed efficienti, infine, offrire servizi migliori e su misura per i clienti.

Altri benefici dell'IA riguarderanno, poi, il settore dei servizi pubblici, in cui si renderanno possibili nuove opzioni, in particolare per la gestione dell'energia e lo smaltimento dei rifiuti, in tal modo contribuendo anche al conseguimento degli obiettivi del "*Green Deal*"[42] europeo. Inoltre, con l'impiego di queste nuove tecnologie la democrazia risulterà rafforzata dalla possibilità di effettuare verifiche basate sui dati, combattere la disinformazione[43], prevenire gli attacchi informatici e, in ultima analisi, garantire l'accesso a informazioni di qualità. Sul piano della sicurezza, in particolare, l'IA costituirà un ausilio prezioso nella prevenzione dei reati. Come supporto nell'esercizio della giustizia penale, poi, essa consentirà di elaborare molto velocemente grandi quantità di dati, in modo da poter prevedere e prevenire crimini e attacchi terroristici, ma anche individuare e contrastare pratiche illegali o inappropriate della rete; in caso di crimini informatici potrà essere utilizzata sia per la difesa, sia per predisporre strategie di attacco contro obiettivi chiave[44].

41. Si veda in Parlamento europeo 2023: "L'economia circolare è un modello di produzione e consumo che implica condivisione, prestito, riutilizzo e riparazione, ricondizionamento e riciclo dei materiali e prodotti esistenti il più a lungo possibile. In questo modo si estende il ciclo di vita dei prodotti, contribuendo a ridurre i rifiuti al minimo"; cfr. anche Commissione europea 2020.
42. Per una sintetica ma efficace presentazione, si veda Commissione europea, *Il Green Deal europeo. Per diventare il primo continente a impatto climatico zero*, 2020.
43. Su questo aspetto particolare si vedano le pagine del sito web del Parlamento europeo dedicate al tema *Disinformazione*.
44. Si veda Consiglio europeo-Consiglio dell'Unione europea 2024. Il Centro europeo per la criminalità informatica (European Cybercrime Centre – EC3), istituito nel 2013, ha fornito un importante contributo alla

Ai sempre più rilevanti e diffusi benefici connessi all'impiego delle tecnologie proprie dell'Intelligenza artificiale corrispondono però anche numerosi rischi, attinenti in particolare: al loro possibile abuso o sottoutilizzo, alla disciplina della responsabilità civile per danni causati da dispositivi o servizi che incorporino funzioni specifiche dell'IA, ma anche alle esigenze di tutela dei diritti fondamentali dell'Unione europea. Gravi minacce, poi, possono sorgere nei confronti della protezione dei dati e per il diritto alla vita privata, come pure per l'esercizio della democrazia e la concorrenza del mercato. Ancora, può essere messa seriamente a repentaglio l'integrità fisica della persona qualora si tratti di applicazioni di IA collocate a contatto o addirittura integrate nel corpo umano, mentre un uso non adeguatamente regolamentato di queste nuove tecnologie negli armamenti potrebbe condurre alla perdita del controllo su di essi, con inimmaginabili conseguenze sugli equilibri internazionali e sulla pacifica coesistenza tra gli Stati.

Molteplici e gravi possono essere, infine, i problemi derivanti dalla mancanza di trasparenza nella struttura e nel funzionamento dei sistemi di IA: le informazioni acquisite possono essere insufficienti, errate o addirittura volutamente distorte, inducendo l'utente a compiere scelte fuorvianti o a prendere decisioni del tutto sbagliate. A seguito dei più recenti sviluppi tecnologici, inoltre, può accadere anche che l'utente non sia in grado di comprendere se stia interagendo con una persona umana ovvero con un sofisticato sistema conversazionale intelligente.

3.2. Il contesto geopolitico e gli obiettivi della politica europea per l'IA

La complessità delle valutazioni relative al necessario bilanciamento tra opportunità e svantaggi nell'introduzione massiccia dell'IA deve poi integrarsi all'interno d'un contesto geopolitico fortemente condizionato dalla presenza dominante dei due principali *competitors* globali: gli Stati Uniti e la Cina. Entrambe orientate verso una decisa incentivazione degli investimenti pubblici e privati nell'IA, queste due potenze hanno in comune il riconoscimento dell'importanza strategica fondamentale del settore, ma anche la preoccupazione di non ostacolarne in alcun modo le dinamiche e lo sviluppo con un apparato normativo di tipo analitico e cautelativo, caratterizzandosi, i primi, per i timori relativi alla tutela dei diritti fondamentali e, la seconda, per l'impostazione disinvoltamente autoritaria di una politica irrispettosa tanto della privacy dei cittadini quanto delle esigenze di trasparenza dei sistemi[45].

Nel quadro normativo statunitense, in materia di regolazione dell'IA è considerata centrale l'importanza della sicurezza e dell'affidabilità dell'innovazione tecnologica in corso. È del 30 ottobre 2023 l'*Executive Order* del Presidente Biden[46], in cui sono enunciati gli otto principi ispiratori della politica che s'intende attuare. A livello federale esistono poi iniziative di legislazione c.d. "orizzontale", relativa cioè a una molteplicità di sistemi di IA rilevanti sul piano decisionale e con possibili ricadute sulla stessa vita degli utenti, ma anche atti di regolazione dell'Intelligenza artificiale generativa, della tecnologia delle risorse umane, nonché delle piattaforme e delle comunicazioni online[47].

Sempre al di fuori dell'Unione europea è qui da segnalare anche la posizione del Regno Unito che, nel 2022, è stato il terzo paese al mondo, dopo gli Stati Uniti e la Cina, a registrare i maggiori investimenti privati e il più alto numero di nuove imprese attive nel settore dell'IA, distinguendosi per l'importanza delle ricerche in svolgimento e l'entità delle risorse pubbliche destinate (*Global AI Index*, Tortoise Media, 2022). L'approccio espresso è manifestamente orientato verso una regolazione

lotta contro la criminalità informatica concorrendo a proteggere i cittadini, le imprese e i governi europei dalla criminalità online.

45. Si vedano, fra gli altri: Burt 2021; Aaronson 2020. Per quanto riguarda la Cina occorre fare riferimento al documento pubblicato dal Consiglio di Stato cinese il 20 luglio 2017, che definisce una progettazione d'alto livello e illustra l'approccio del paese allo sviluppo della tecnologia e delle applicazioni dell'IA, stabilendo obiettivi generali validi fino al 2030. Cfr. Consiglio di Stato cinese 2017. Si vedano, fra gli altri: Roberts–Cowls–Morley et al. 2021; Khanal–Zhang–Taeihagh 2024.
46. Si veda Sulmicelli 2023.
47. Si veda Anand 2024.

prudente ma flessibile, attenta all'esigenza di non limitare o imbrigliare gli sviluppi della nuova tecnologia, fornendo indicazioni chiare e tempestive all'industria e nel contempo promuovendo l'interoperabilità a livello internazionale. In questa prospettiva la regolazione, pur essendo considerata d'importanza primaria, non si configurerebbe sempre come lo strumento più efficace per promuovere e sostenere un'innovazione responsabile, essendo invece necessario il ricorso a varie forme d'integrazione, basate sull'osservanza di princìpi fondamentali come l'equità, la sicurezza e la protezione, la trasparenza e la contestabilità, la responsabilità e la governance. All'implementazione di tali princìpi dovranno provvedere le Autorità già esistenti, mentre eventuali modifiche e aggiustamenti potranno derivare dall'esecuzione di test e sperimentazioni in ambienti controllati, ma anche dallo svolgimento di consultazioni pubbliche.

Il 1° aprile 2024, gli Stati Uniti e il Regno Unito hanno firmato un *memorandum of understanding* sull'Intelligenza artificiale[48], che costituisce il primo accordo bilaterale al mondo relativo alla valutazione e allo studio dei rischi connessi all'IA. In forza dell'accordo raggiunto Stati Uniti e Regno Unito collaboreranno mettendo reciprocamente a disposizione le proprie conoscenze scientifiche in ordine all'implementazione di modelli di IA sicuri: in concreto l'US AI Safety Institute (US AISI) e l'omologo Istituto britannico potranno condividere informazioni attinenti alla sicurezza dei modelli di IA e quindi ai rischi a essi associati, in modo da sviluppare alcuni approcci metodologici volti ad affrontarli e limitarli.

L'analisi, sia pur sommaria, del contesto geopolitico in cui l'Unione si trova inserita consente di comprendere agevolmente per quali motivi l'Europa abbia dovuto affrontare con urgenza il problema di realizzare una disciplina normativa del fenomeno complessivo dell'IA: si tratta di entrare in una difficile, ma necessaria competizione con i Paesi tecnologicamente più avanzati, creando un ambiente favorevole alla ricerca e allo sviluppo, assicurando e stimolando i necessari investimenti, ma nel contempo mantenendo salda l'esigenza di riaffermare e tutelare quei diritti fondamentali, quei valori e quei principi su cui l'Europa stessa si fonda.

L'obiettivo principale della politica europea è dunque duplice: da una parte, garantire all'Ue la possibilità di acquisire e mantenere una leadership mondiale in questo campo, facendo però in modo che l'impiego dell'IA avvenga nel pieno rispetto dei diritti fondamentali, dei princìpi e dei valori europei; dall'altra, assicurarsi che la regolazione europea dell'IA risulti equilibrata, idonea a contemperare concezioni ed esigenze diverse (talora perfino tra loro contrastanti), proporzionata rispetto ai rischi da evitare o limitare, atta a incoraggiare e promuovere lo sviluppo tecnologico suscitando e garantendo la fiducia di cittadini e utenti, flessibile e adattabile nei confronti dei rapidi e continui cambiamenti che caratterizzano queste tecnologie, assicurando nel contempo anche quel grado di certezza e prevedibilità che è essenziale in un settore tanto strategico e delicato. Si tratta, evidentemente, di un equilibrio non facile da trovare a livello nazionale né, tantomeno, a livello europeo (o globale): le regole sono necessarie per assicurare il rispetto dei diritti e dei valori su cui si basa l'Unione europea, ma non devono costituire un ostacolo rispetto a quello sviluppo scientifico, economico e sociale che l'IA può produrre[49].

Agli obiettivi fin qui chiariti deve ovviamente corrispondere un ambito d'applicazione particolarmente esteso: per esplicare concretamente la loro efficacia le nuove norme dovranno applicarsi non solo all'immissione sul mercato, ma anche alla messa in servizio e all'uso dei "sistemi di IA", intesi, in senso ampio, come software sviluppati con tecniche specificamente indicate e idonei a generare contenuti, previsioni, raccomandazioni o decisioni, tali da poter influenzare l'ambiente con cui interagiscono[50]. Le nuove norme dovranno poi essere

48. Si veda U.S. Department of Commerce, Office of Public Affairs 2024.

49. Per un confronto tra la strategia USA e quella europea cfr. Chiti–Marchetti 2020; Cath–Watcher–Mittelstadt et al. 2018.

50. Nel testo inglese della Proposta di Regolamento la definizione dei "sistemi di IA" è così espressa: "Artificial Intelligence system (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

applicate direttamente, allo stesso modo, in tutti gli Stati membri, sulla base di una definizione dell'Intelligenza artificiale[51] sufficientemente flessibile e comprensiva, atta ad esprimerne la complessità concettuale e le potenzialità di sviluppo, ma allo stesso tempo accompagnandone la rapida evoluzione.

4. La Legge europea sull'Intelligenza artificiale (AI Act): entrata in vigore e ambito di applicazione

Il 13 marzo 2024 il Parlamento europeo ha approvato, con ampia maggioranza, il Regolamento sull'Intelligenza artificiale (AI Act)[52]; a poco più di due mesi di distanza, il 21 maggio successivo, è giunta anche l'approvazione del Consiglio dell'Unione europea[53]. La pubblicazione nella Gazzetta Ufficiale dell'Unione è avvenuta il 12 luglio 2024[54].

Dopo venti giorni, in data 1° agosto 2024, la legge è entrata finalmente in vigore, ma comincerà a essere applicata solo dopo 24 mesi[55]. Sono comunque previste alcune eccezioni: le regole relative ai sistemi di IA vietati si applicano 6 mesi dopo l'entrata in vigore; i codici di buone pratiche, 9 mesi dopo; le norme sui sistemi di IA per finalità

51. La definizione dell'Intelligenza artificiale, elaborata dal "Gruppo indipendente di esperti di alto livello sull'Intelligenza artificiale" (*High Level Expert Group on Artificial Intelligence* – AI HLEG) nominato dalla Commissione europea, era così espressa: "I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti".
52. Il testo del Regolamento contenente le proposte di emendamento, frutto dell'accordo raggiunto con gli Stati membri nel dicembre 2023, dopo avere ottenuto l'approvazione del "Comitato dei rappresentanti permanenti degli Stati membri" (COREPER), della "Commissione per le libertà civili, la giustizia e gli affari interni" (LIBE) e della "Commissione per il mercato interno e la protezione dei consumatori" (IMCO), è stato approvato dai deputati europei con 523 voti favorevoli, 46 contrari e 49 astensioni.
53. Il testo del "Regolamento recante norme armonizzate sull'Intelligenza artificiale" (Legge sull'Intelligenza artificiale) è stato approvato, insieme, dal Parlamento europeo e dal Consiglio dell'Unione europea in data 21 maggio 2024.
54. Il testo pubblicato nella Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024 reca il titolo "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)". La cronologia storica dell'AI Act è presentata nella Historic Timeline del Future of Life Institute. Per una presentazione complessiva della legge si vedano, tra i tanti: Alaimo 2023; Barbaja 2024; Bocchini 2024; Capacci–Galli–Loreggia–Maroccia 2024; Iaselli 2024; Lalli 2024, Voigt–Hullen 2024. Per agevolare l'analisi del testo – molto esteso, comprendendo 180 considerando, 113 articoli distribuiti in 13 Capi e 13 Allegati – sono stati già implementati alcuni utili strumenti di navigazione. Tra questi si possono qui citare: l'*AI Act Explorer*, sviluppato dal "Future of Life Institute"; ClaiRK, strumento articolato che consente d'effettuare anche ricerche testuali e semantiche, realizzato dal "Digital Policy Alert team"; Lexroom AI Act, nuovo modulo della piattaforma Lexroom.ai, progettato da una giovane start-up innovativa in modo da poter rispondere a domande in linguaggio naturale in merito ai contenuti della legge europea sull'Intelligenza artificiale, fornendo in pochissimo tempo una "bozza di parere" o una "risposta pragmatica", ma anche citando e allegando le fonti giuridiche utilizzate. Infine, un indice interattivo dell'AI Act è stato prodotto anche dal MIAI (*Multidisciplinary Institute in Artificial Intelligence*) dell'Université Grenoble Alpes.
55. Il Regolamento europeo sull'IA, come tutti i regolamenti dell'Ue, è un atto normativo di carattere generale, vincolante e direttamente applicabile; essendo *self executive*, non richiede alcuna legge di recepimento, ma entra direttamente a far parte del corpo legislativo nazionale di ciascuno Stato membro.

generali (*General Purpose AI* – GPAI), compresa la governance, 12 mesi dopo; infine, gli obblighi per i sistemi di IA ad alto rischio entreranno in vigore solo dopo tre anni, mentre il periodo di tolleranza è esteso a ben quattro anni per i sistemi IA ad alto rischio che siano in uso da parte di pubbliche autorità e immessi sul mercato prima dell'entrata in vigore della legge. Gli Stati membri, poi, hanno 12 mesi di tempo per creare un'Autorità locale di notifica e di sorveglianza del mercato, ma potranno disporre di due anni per approntare le regolamentazioni locali[56].

Come già precisato, l'AI Act tende a garantire che i sistemi di IA immessi sul mercato europeo siano sicuri e rispettino i diritti e i valori fondamentali dell'Unione europea; nel contempo, però, esso si propone anche di stimolare gli investimenti e l'innovazione nel settore dell'Intelligenza artificiale, agevolando lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili. Norme nazionali diverse in ognuno dei singoli Stati membri, infatti, porterebbero alla frammentazione del mercato interno, mettendone a rischio il vantaggio competitivo e pregiudicando la necessaria certezza del diritto nei confronti di quanti sviluppino, producano, utilizzino o importino sistemi di IA all'interno dell'Unione.

A livello comunitario, relativamente a una materia tanto complessa oltre che in continua evoluzione, si rende evidente la ferma volontà d'inserire nella legislazione europea una disciplina organica e unitaria, tale da poter diventare non solo un punto di riferimento cogente per le legislazioni degli altri Stati membri, ma anche un prototipo normativo suscettibile d'essere assunto come modello cui ispirarsi per i Paesi al di fuori dell'Unione.

Il testo del Regolamento approvato dal Parlamento europeo e dal Consiglio dell'Unione conferma l'approccio basato sul rischio, già adottato nelle precedenti versioni. Pertanto, sono imposti obblighi diversificati in base al livello di rischio che ciascuna delle categorie in cui si possono classificare i sistemi di IA può comportare nei confronti dei diritti e delle libertà personali: da un rischio inaccettabile si passa alla configurazione di un rischio alto e, successivamente, basso o minimo.

Rispetto alla Proposta presentata dalla Commissione il 21 aprile 2021[57], nel quadro normativo che emerge dal testo definitivo della legge sull'Intelligenza artificiale sono principalmente evidenziabili: le nuove disposizioni relative ai modelli di IA a carattere generale ad alto impatto; la ridistribuzione dei poteri in ambito istituzionale, con una più forte centralizzazione delle decisioni esecutive a livello sovranazionale; l'introduzione di nuove pratiche vietate connesse all'uso di sistemi di IA; le precisazioni introdotte in riferimento alle situazioni in cui l'impiego di sistemi d'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico si rende strettamente necessario per il contrasto alla criminalità; infine, la valutazione d'impatto, preliminare all'attivazione di un sistema di IA.

Le regole armonizzate stabilite nel Regolamento sono state concepite in modo da non pregiudicare la normativa vigente dell'Unione, in particolare in materia di diritti fondamentali, protezione dei

56. Si riporta qui di seguito lo scadenzario dettagliato previsto dal legislatore per l'entrata in vigore e l'applicazione della legge (art. 113): l'entrata in vigore della legge sull'AI è avvenuta 20 giorni dopo la pubblicazione nella Gazzetta ufficiale dell'Unione europea, il 1° agosto 2024; dal 2 febbraio 2025 si applicheranno i Capi I (disposizioni generali) e II (sistemi di IA vietati); dal 2 agosto 2025 si applicheranno il Capo III, Sezione 4 (Autorità di notifica), il Capo V (modelli di IA per scopi generali), il Capo VII (governance), il Capo XII (riservatezza e sanzioni) e l'articolo 78 (riservatezza), ad eccezione dell'articolo 101 (sanzioni per i fornitori di IA *general purpose*); dal 2 agosto 2026 si applicherà l'intera legge sull'IA, ad eccezione dell'articolo 6 (regole di classificazione per i sistemi di IA ad alto rischio), paragrafo 1, e degli obblighi corrispondenti; dal 2 agosto 2027 si applicheranno l'articolo 6, paragrafo 1, e gli obblighi corrispondenti. Per un'analisi dettagliata si veda Zorloni 2024.

57. La Proposta di Regolamento sull'Intelligenza artificiale presentata dalla Commissione europea il 21 aprile 2021 [COM(2021) 206], mirando a stabilire regole comuni atte a salvaguardare i diritti umani fondamentali e allo stesso tempo agevolare lo sviluppo del mercato interno, forniva una definizione e classificazione dei sistemi di IA, indicava i requisiti obbligatori per la loro progettazione e realizzazione, commercializzazione e utilizzo, prevedendo anche diversi strumenti di controllo e uno specifico apparato sanzionatorio.

dati, tutela dei consumatori, sicurezza dei prodotti, occupazione e protezione dei lavoratori.

Sotto il profilo soggettivo, in base all'art. 2 la legge si applica agli utilizzatori dei sistemi di IA, siano essi enti pubblici o privati, ma anche ai fornitori, ai *deployer*, agli importatori, ai distributori, ai fabbricanti, ai rappresentanti autorizzati e, in generale, a quanti siano comunque coinvolti nell'uso di tali sistemi. Nel successivo art. 3 sono fornite le definizioni relative alle figure di "fornitore" ("provider"), "deployer", "rappresentante autorizzato", "importatore", "distributore" e "operatore". Sul piano pratico è qui da rilevare l'importanza della corretta individuazione della qualifica attribuibile al soggetto, in quanto da essa discende l'attribuzione d'un insieme di obblighi e responsabilità. In particolare, com'è stato osservato[58], in considerazione del fatto che tali obblighi e responsabilità sono per la maggior parte normativamente previsti a carico del provider, la distinzione tra la figura di "provider" e quella di "deployer" – che sovente può risultare difficile a causa del notevole livello di personalizzazioni che le aziende tendono ad apportare ai sistemi – e la conseguente corretta attribuzione della corrispondente qualifica comportano conseguenze pratiche rilevanti.

Per quanto attiene al criterio della territorialità, l'AI Act ha adottato una soluzione simile a quella utilizzata dal GDPR e da altre normative in materia di tecnologie digitali: esso, infatti, trova applicazione non solo con riferimento ai fornitori di sistemi di IA che li immettono sul mercato o li utilizzano nel territorio dell'Unione europea, ma anche nei confronti di quanti operano al di fuori di tale ambito se i risultati generati da tali sistemi sono poi comunque utilizzati in Europa. La *ratio* della norma, dunque, estendendo la sua applicabilità anche a soggetti esterni all'Unione, funziona come misura protettiva, nel senso di prevenire l'introduzione e la commercializzazione nel mercato dell'Ue di sistemi di Intelligenza artificiale che abbiano caratteristiche intrinseche o ricadute pratiche del tutto difformi dai principi e valori su cui si fonda la legislazione europea.

Il Regolamento non sarà invece applicabile a settori che non rientrino nell'ambito di applicazione del diritto dell'Unione, non pregiudicando in ogni caso le competenze degli Stati membri in materia di sicurezza nazionale. In sintesi, esso non si applicherà: a) ai sistemi di IA che hanno scopi militari, di difesa o di sicurezza nazionale (indipendentemente dal tipo di entità che svolge tali attività); b) ai sistemi o modelli di IA sviluppati e utilizzati esclusivamente per scopi di ricerca e innovazione; c) ai sistemi rilasciati con licenze free e open source, a meno che non siano collocati sul mercato o immessi in servizio come sistemi ad alto rischio; d) infine, alle persone fisiche che utilizzino l'IA nel corso di attività non professionali, meramente personali.

5. Considerazioni finali: ultimi sviluppi dell'Intelligenza artificiale e prime valutazioni dell'AI Act

L'AI Act ha il grande merito di porsi come prima esperienza, a livello mondiale, nella regolazione complessiva e organica del fenomeno dell'Intelligenza artificiale. Nella prima parte della trattazione si è cercato di evidenziare il significato e la portata della rivoluzione che l'IA di nuova generazione (la c.d. "New Generation AI") sta massicciamente introducendo non solo nella società in cui viviamo – nei suoi diversi profili, come pure in tutte le attività che in essa si svolgono –, ma perfino negli aspetti più privati della nostra vita individuale. Nell'analisi del rapporto tra uomo e computer, prendendo atto della rivoluzione tecnologica in corso, si è evidenziata la necessità di acquisire consapevolezza del fatto che si sono aperti scenari assolutamente nuovi e in gran parte imprevedibili. Il computer non è più la macchina inerte che si limita a eseguire, in modo rigido e sequenziale, gli ordini impartitigli dal programmatore: la "capacità di apprendimento" (*machine learning*) di cui può essere dotato, lo trasforma in interlocutore attivo, in grado non solo di

58. Le definizioni di "fornitore" (provider) e "distributore" (deployer) sono contenute nell'art. 3 dell'AI Act. Unitamente all'individuazione della classe di rischio cui appartiene il sistema di AI volta a volta in esame, l'esatta identificazione di questi due ruoli distinti, ma a volte intersecantisi, proprio per le conseguenze giuridiche che ne derivano, costituisce uno dei problemi centrali nell'applicazione dell'AI Act. Si vedano, tra gli altri: Coraggio 2024; Cavazzuti 2024; De Leo–Biscaretti di Ruffia 2024; Stefanelli–Terrizzi 2024; Gui–Ivankovich–Mancini et al. 2024; *Deployment*, Voce in "Wikipedia. L'enciclopedia libera".

registrare enormi masse di dati, ma anche di elaborarle in modo da estrarne nuova conoscenza (*data mining*) e, quindi, di conseguire un'esperienza sulla cui base formulare proposte d'azione o, addirittura, prendere autonome decisioni.

Il legislatore europeo, già nel corso della lunga e faticosa elaborazione della sua proposta regolatoria sull'IA, si è trovato a dover affrontare problematiche del tutto nuove o comunque non assimilabili a esperienze normative anche recenti. In particolare, le sempre più numerose e varie applicazioni dell'Intelligenza artificiale generativa (*Generative AI*), che utilizzano algoritmi complessi al fine di creare in modo autonomo (senza l'intervento dell'uomo) nuovi contenuti (non solo testi, ma anche immagini, video, musica), hanno reso necessaria, rispetto all'originaria stesura della Proposta di regolamento da parte della Commissione, l'introduzione d'un complesso insieme di norme in materia di "Modelli di IA per finalità generali" e "Modelli di IA con finalità generali con rischio sistemico" (Regolamento (UE) 2024/1689, Capo V, Sezione 1).

Non si tratta semplicemente dell'utilizzo di nuovi strumenti e di nuove forme d'interazione con la macchina, bensì dell'avvio di una nuova era, contrassegnata da un radicale "cambiamento della nostra architettura cognitiva". Quando si interagisce in maniera non superficiale con sistemi di IA è infatti inevitabile riscontrare mutamenti anche nel proprio modo di affrontare i problemi, sollevando dubbi, formulando (e ponendosi) domande, individuando alternative, analizzando e collegando risposte. Gradatamente, ma irreversibilmente, si sta configurando – e rapidamente estendendo – una nuova forma di pensiero che potrebbe qualificarsi come "ibrida", in quanto in essa si rapportano e si integrano la vastità dei dati che la macchina è in grado d'acquisire ed elaborare, da una parte, e la sensibilità umana, la imprevedibilità dell'intuizione, la maturazione indotta dall'esperienza, dall'altra[59].

In considerazione della continua e veloce evoluzione della tecnologia in questo campo, la materia oggetto di regolazione nell'AI Act risulta essersi già ampliata e modificata. Dopo l'ascesa della "IA generativa", infatti, l'IA è sull'orlo di un'altra significativa trasformazione con l'avvento della "IA agentica" (*Agentic AI*). Si tratta di un cambiamento indotto dall'evoluzione dei *Large Language Models* (LLM) in entità attive e decisionali, in grado non solo di generare testi simili a quelli prodotti dall'uomo, ma anche di ragionare, pianificare, usare strumenti ed eseguire autonomamente attività complesse. Questa evoluzione, ridefinendo il modo in cui interagiamo con l'IA, segna l'inizio di una nuova era nell'ambito delle modalità di configurazione e delle possibilità di utilizzo delle corrispondenti tecnologie. L'IA agentica si riferisce a sistemi o agenti che possono svolgere compiti in modo indipendente (senza una guida umana costante), adattandosi anche a situazioni mutevoli. A differenza dei sistemi di IA convenzionali, limitati a compiti fissi, l'IA agentica è dinamica, impara dalle interazioni, migliora progressivamente il suo comportamento nel tempo e ha la capacità di suddividere i compiti in passaggi più semplici, analizzando diverse soluzioni alternative e prendendo decisioni sulla base di obiettivi, istruzioni o *feedback*[60].

È evidente che il legislatore europeo dovrà prendere sollecitamente in considerazione queste nuove potenzialità emerse nell'ambito dell'IA, in modo da valutarne, sotto i diversi profili giuridici, la varietà delle forme applicative, così come la gravità dei rischi connessi. Rimanendo entro i confini assegnati alla presente trattazione è possibile in questa sede solo accennare a quelle tendenze evolutive che, secondo quanto autorevolmente affermato[61], sono ormai prossime a trasformare

59. In generale, sulle tendenze di sviluppo dell'IA si veda Martino 2024. Una panoramica dettagliata delle sfide, delle prospettive e dei rischi legati all'Intelligenza artificiale in vari ambiti (calcolo, big data, gioco, scrittura, etica, tag, lavoro, guerra, cervello, futuro) è presentata nel volume *Intelligenza artificiale. Dieci ambiti della nostra vita che stanno cambiando per sempre*, pubblicato, con la collaborazione degli editor della rivista "Internazionale" D. Cassandro e P. Romano, per BUR da Mondadori, 2024.

60. Sulla "Intelligenza artificiale agentica" si vedano, tra gli altri: Zia 2024; Viliotti 2024; Chudleigh 2024.

61. Si veda Studio Gartner 2024. Sulla "originalità" della conoscenza prodotta dalla IA generativa e sul dialogo come forma di interazione tra l'uomo e la macchina, ma anche come fonte di nuova conoscenza si veda Martino 2024.

radicalmente la società, soprattutto sotto il profilo del rapporto uomo-macchina. La GenAI ("AI generativa") di tipo multimodale (testo, immagine, audio e video), i "Modelli GenAI specifici per il dominio" e gli "Agenti autonomi" sono stati identificati come tecnologie ad alto impatto trasformativo generale, essendo in grado di offrire, tra l'altro, maggiore precisione, trasparenza, sicurezza e privacy[62]. In generale, poi, l'integrazione dell'AI generativa nelle attività di aziende, professionisti e utenti comuni è diventata una tendenza in forte crescita, evidenziando un impatto senza precedenti nella storia delle innovazioni tecnologiche. A ciò si aggiunga ancora che l'industria degli smartphone e dei computer si è rivolta con ottimismo all'Intelligenza artificiale come a un catalizzatore d'innovazione: si prevede che i primi smartphone con AI integrata sui chip miglioreranno radicalmente l'esperienza degli utenti, offrendo assistenti vocali più intelligenti e App in grado d'eseguire compiti complessi.

La sensibilizzazione ai numerosi profili giuridici presentati nell'AI Act dovrebbe indurre a perseguire non solo il potenziamento dei processi di AI, ma anche la loro trasparenza e comprensibilità. In tale contesto si inserisce la c.d. "Intelligenza artificiale spiegabile" (XAI – *Explainable Artificial Intelligence*): si tratta di un'area di ricerca in rapida crescita che si è posta come obiettivo il miglioramento della interpretabilità dei modelli di AI, sovente percepiti come vere e proprie "scatole nere". Rendere i sistemi di IA non solo precisi e funzionali, ma anche comprensibili per gli utenti genera fiducia e sicurezza, oltre a costituire la necessaria premessa per una documentata valutazione di conformità[63].

Sempre con riferimento alle nuove sfide che la regolazione giuridica dell'IA deve affrontare occorre tener presente anche che, molto di recente, si stanno realizzando ulteriori progressi nel senso del superamento della stessa IA generativa: si tratta dell'emergere di sistemi di IA di tipo non solo "generativo", ma anche "evolutivo". Sotto il profilo metodologico un esempio rilevante e concreto di questa transizione verso la "IA evolutiva" è costituito dalla tecnologia "FunSearch" (abbreviazione di "ricerca nello spazio delle funzioni"), sviluppata da Google DeepMind: partendo dalla descrizione di un problema in forma di codice informatico, la procedura ne cerca la soluzione utilizzando la creatività dei *Large Language Models* (LLM) in associazione con un sistema di verifica dell'efficacia delle idee proposte (valutatore sistematico). La particolarità di questa strategia – che rappresenta anche un modello per i futuri sviluppi delle tecnologie nel campo della IA – risiede nell'approccio iterativo, in cui si combinano un'Intelligenza artificiale creativa e una procedura che verifica l'efficacia delle soluzioni proposte[64].

Notevoli problemi, non solo di natura giuridica, ma anche economica, sociale ed etica, si ricollegano, poi, ai recenti sviluppi della robotica. Progetti come KnowNo[65], che nella loro configurazione integrano l'Intelligenza artificiale generativa consentendo la realizzazione di robot in grado di "sapere quando non sanno" e quindi di chiedere aiuto solo quando ciò risulti necessario, segnano già l'inizio di una nuova era relativamente al modo in cui queste macchine interagiscono col mondo fisico ed effettuano scelte. Il superamento dei metodi tradizionali di programmazione in questo settore particolare rappresenta un passo significativo verso un futuro in cui i robot non saranno più strumenti passivi, bensì partner affidabili, capaci di operare anche in ambienti dinamici e non strutturati, oltre che di partecipare attivamente nel risolvere problemi e prendere decisioni.

A conclusione di questa rassegna – sia pure superficiale e lacunosa – delle più recenti tendenze evolutive dell'IA, considerate nella prospettiva dei necessari interventi regolatori del legislatore, tra le numerose trasformazioni indotte dalla tecnologia nella struttura sociale e negli ambienti di lavoro occorre accennare anche al fenomeno

62. Una sintetica presentazione delle tecnologie da ultimo citate nel testo è in AI4Business (Red.) 2024.

63. Un'analisi della *Explainable Artificial Intelligence*, condotta con l'intento di promuovere la discussione collaborativa e la cooperazione interdisciplinare, è in Longo–Brcic–Cabitza et al. 2024. Presentazioni più semplici e sintetiche sono in Do Couto 2024; IBM (Red.) 2020. Un'ampia bibliografia è riportata in *Explainable artificial intelligence*, Voce in "Wikipedia. L'enciclopedia libera".

64. Si veda Fawzi–Romera-Paredes 2023; Romera-Paredes–Barekatain–Novikov et al. 2024; Mouret 2024.

65. Si veda Ren–Dixit–Bodrova et al. 2023; Viliotti 2023.

conosciuto come BYOAI (acronimo di *Bring Your Own Artificial Intelligence*). In uno scenario del genere i dipendenti di un'azienda, per svolgere i compiti loro assegnati, utilizzano strumenti e applicazioni di IA esterni al proprio contesto lavorativo, indipendentemente dal fatto che tali strumenti siano o meno ufficialmente approvati dall'azienda stessa. Com'è agevole intuire, questa tendenza, alimentata dalla crescente disponibilità di sistemi di IA a basso costo e di semplice utilizzo, fa sorgere notevoli problemi giuridici riguardanti soprattutto la governance organizzativa e la valutazione della conformità normativa, ma anche il controllo e la sicurezza dei dati, il rispetto del copyright e la tutela della privacy[66].

L'AI Act, come già rilevato, costituisce il primo tentativo, a livello mondiale, di regolazione normativa dell'Intelligenza artificiale e delle sue estremamente numerose e differenti applicazioni. Nello svolgimento della presente trattazione si è cercato di mettere in luce le caratteristiche essenziali e lo sconvolgente potenziale trasformativo di questo fenomeno del tutto nuovo nella storia dell'intera umanità. Si è reso evidente che, da un lato, i molteplici problemi sollevati richiedono interventi tempestivi; dall'altro, proprio in funzione dei delicati e complessi equilibri che si rischia di compromettere, le iniziative regolatorie necessitano di un'attenta ponderazione, ma anche di una costante rivalutazione.

Anche a un livello d'analisi superficiale, in prima istanza risulta assai arduo definire i confini della materia da regolare, in considerazione dell'attuale sempre più spinta pervasività dell'IA, ma anche dell'impressionante molteplicità e varietà delle sue applicazioni. Ogni tipologia d'utilizzo – spaziando senza limiti (ed esemplificando in maniera del tutto casuale) dalla medicina alla finanza, dalla ricerca scientifica all'organizzazione aziendale, dalla mobilità all'assistenza legale – coinvolge numerose specializzazioni, sovente distanti tra loro e non sempre agevolmente reperibili. Non solo; ad ogni contesto applicativo corrispondono problematiche differenti, di tipo sociale, giuridico ed etico. A tutto ciò si aggiunga il fatto che se, da una parte, appare estremamente complesso individuare con esattezza l'oggetto della normazione, dall'altra, sotto il profilo temporale il legislatore si trova nell'impossibilità di prevedere e fronteggiare gli sviluppi della tecnologia, in considerazione dell'impressionante velocità del progresso scientifico del settore, ma anche del continuo superamento di limiti che solo poco tempo prima sembravano invalicabili.

Tra l'altro, lo sviluppo esplosivo dell'IA ha incluso anche un processo di "democratizzazione", coinciso con il lancio, nel 2023, di "ChatGPT", un chat-bot AI che, sfruttando l'Intelligenza artificiale generativa e l'apprendimento automatico e basandosi su un modello conversazionale, è in grado di dialogare con l'utente finale e creare non solo testi, ma anche immagini, audio e video[67]. A livello mondiale migliaia di sistemi di IA fondati sulle tecnologie di OpenAI, Google AI e Microsoft si stanno rapidamente diffondendo. Inoltre, Google ora integra la propria Intelligenza artificiale in tutte le App e, allo stesso modo, Microsoft utilizza la sua IA in tutti i programmi, compresi quelli che fanno parte di Microsoft Office. Anche molte terze parti, tra cui importanti reti social come Linkedin, stanno integrando l'IA nelle loro piattaforme. Occorre rilevare, però, che, rispetto a questa realtà, sembra mancare, o essere comunque carente e non aggiornata, la competenza dei politici e dei legislatori, nei Parlamenti nazionali come a livello europeo.

Probabilmente proprio a causa delle difficoltà indicate, derivanti dai labili confini dell'Intelligenza artificiale e dalla rapidità della sua evoluzione, l'AI Act si presenta come un documento molto lungo, complesso e sovente di difficile interpretazione. Il testo normativo comprende 180 considerando, 113 articoli (organizzati in 13 Capi e talora tanto estesi da dover essere suddivisi in paragrafi, commi, numeri, lettere e punti[68]) e 13 Allegati. Inoltre, sono molto numerose le disposizioni di rilievo sostanziale che dovranno essere definite solo in atti legislativi e regolamentari successivi, la

66. Si vedano van der Meulen–Wixom 2024, Marr 2024.

67. Molto popolare in Italia fin dal suo debutto, ChatGPT ha riscosso ampi consensi tra gli italiani, che risultano tra i primi 10 utenti al mondo per volume di ricerche. L'ultima versione, denominata GPT-40, è stata presentata il 13 maggio 2024. Si veda Castigli–Sandonnini 2024.

68. Si vedano, ad esempio, l'art. 3, contenente ben 68 definizioni esplicative di espressioni e termini tecnici utilizzati nella legge, e l'art. 5, che enumera le "Pratiche di IA vietate".

cui emanazione è posta a carico della Commissione[69]. A questi occorre poi aggiungere le norme con cui i 27 Stati membri recepiranno il Regolamento. Il rinvio ad atti successivi può apparire come un'opportuna scelta di flessibilità, uno strumento idoneo a fronteggiare una tecnologia in continua e rapida evoluzione, ma rende comunque manifesta la difficoltà d'imbrigliare una materia assai vasta e complessa in un unico atto normativo. Ovviamente, le modalità con cui la Commissione e gli Stati membri applicheranno in concreto le disposizioni del Regolamento andranno poi a incidere sulla valutazione complessiva dell'efficacia della legge.

Sul piano pratico, però, il problema di fondo, uniformemente evidenziato da studiosi e ricercatori, come da imprenditori, economisti e politici, risiede nella situazione di grave ritardo in cui l'Europa versa nei confronti dei principali *competitor* mondiali nel campo dell'Intelligenza artificiale. Nel decennio 2013-2023 risultano oltre 5.500 società specializzate in IA fondate negli Stati Uniti: si tratta d'un numero 4 volte superiore alla Cina, ma addirittura superiore rispetto a quello di tutti gli altri Paesi messi insieme[70]. In Europa ci sono tuttora pochissime aziende in questo settore e mancano, o sono del tutto insufficienti, alcune delle infrastrutture e delle componenti critiche fondamentali (*cloud computing, cybersecurity*, produzione di microchip). In un contesto del genere l'AI Act potrebbe rappresentare il tentativo, da parte dell'Europa, di condizionare mediante una rigida normativa la corsa di Stati Uniti e Cina, nell'impossibilità di concorrere con loro sul piano degli investimenti e dello sviluppo tecnologico. È essenziale, invece, che l'Europa scenda decisamente in campo non solo come arbitro di una competizione tra le due superpotenze, ma soprattutto come protagonista di una sfida irrinunciabile, nella concreta prospettiva dell'acquisizione, in un futuro non lontano, di una leadership globale: aumentare gli investimenti pubblici e privati in ricerca e innovazione all'interno di un efficiente coordinamento europeo dovrebbe portare a creare, in tempi rapidi, la massa critica necessaria a consentire una partecipazione attiva al dialogo e al confronto.

Le critiche prontamente mosse da più parti all'AI Act riguardano molti aspetti della vasta problematica emergente, spaziando, per citarne solo alcune, dai contrasti rilevabili con le precedenti normative europee di settore alla vaghezza di certe definizioni, dalle difficoltà – soprattutto per le piccole e medie imprese – di rispettare meccanismi regolatori costosi e complessi alla pesante incidenza del sistema sanzionatorio, dalla possibilità di esercitare un controllo effettivo sul contenuto dei dataset utilizzati per l'addestramento degli algoritmi alle insidie nascoste nella capacità di "allineamento" delle risposte del programma alle domande e alle attese dell'utente. Le accuse più pesanti e coinvolgenti riguardano, però, proprio la materia dei diritti fondamentali. La nuova legge sull'IA è giudicata da alcuni piena di concessioni alle lobby della grande industria del settore[71], avendo accolto esenzioni relative agli usi più pericolosi dell'IA soprattutto da parte delle forze dell'ordine e delle autorità per la migrazione, e contenendo divieti che, in quanto includono numerose eccezioni e scappatoie, in realtà finirebbero col non vietare alcuni degli usi più pericolosi delle nuove tecnologie, come quello relativo ai sistemi d'identificazione biometrica remota in tempo reale, in spazi accessibili al pubblico e a fini di attività di contrasto[72].

Queste sintetiche osservazioni evidenziano il problema centrale di fronte al quale si è trovato il legislatore europeo: si trattava, da una parte, di mettere l'Unione in condizioni di svolgere un ruolo da protagonista nella scena mondiale della rapidissima trasformazione tecnologica in atto, dall'altra, di garantire comunque la tutela di quei valori e principi su cui l'Unione stessa si fonda.

69. È stato calcolato che le espressioni "*delegated act*" (decreti delegati, che richiedono l'approvazione del Parlamento) e "*implementing act*" (regolamenti, che non richiedono la successiva approvazione del Parlamento) compaiono, rispettivamente, ben 34 e 39 volte. Si veda Capacci–Galli–Loreggia–Maroccia 2024.

70. Si veda D'Ascenzo 2024.

71. Per una sintetica rassegna delle principali criticità evidenziate nell'AI Act, si vedano, tra gli altri: Access Now (Red.) 2023; Bender 2023; Vranken 2023; Alfieri 2024; Bonavita–Cortina 2024; Cirone 2024; De Bree 2024; Panetta 2024; Ponti 2024; Sandonnini 2024; Speroni di Fenizio 2024; Mele 2025.

72. Si veda, in proposito, all'interno dell'AI Act, l'art. 5, par. 1, primo comma, lettera h e, più in generale, la fitta rete di rinvii interni ed esterni che integrano il complesso meccanismo di limitazioni e controlli.

Quanto il difficile contemperamento di queste distinte esigenze sia di fatto riuscito deve essere certamente oggetto d'analisi approfondite, il più possibile esenti da pregiudizi e condizionamenti ideologici. In chiusura ci si limita qui a richiamare le direttive indicate dall'UNESCO nella sua Raccomandazione sull'etica dell'Intelligenza artificiale, volta a fornire standard globali per massimizzare i benefici dell'innovazione tecnologica, assicurando che essa contribuisca realmente a costruire un mondo più inclusivo, sostenibile e pacifico[73].

Riferimenti bibliografici

S.A. Aaronson (2020), *America's uneven approach to AI and its consequences*, in "Institute for International Economic Policy Working Paper Series", George Washington University, April 2020

Access Now (Red.) (2023), *The EU should regulate AI on the basis of rights, not risks*, in "Access Now", 17 February 2021 (last updated: 13 January 2023)

AI4Business (Red.) (2024), *Gartner: entro il 2027 il 40% delle soluzioni di AI generativa sarà multimodale*, in "AI4Business", 9 settembre 2024

A. Alaimo (2023), *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in "federalismi.it", 2023, n. 25

G. Alfieri (2024), *Intelligenza artificiale, chi critica e perché l'AI Act Ue*, in "Startmag", 14 marzo 2024

V. Allis (1994), *Searching for Solutions in Games and Artificial Intelligence*, Ph.D. Thesis, Maastricht University, 1994

N. Anand (2024), *US Federal AI Legislation in 2024: The Current Landscape*, in "Holistic AI", March 8 2024

M. Barbaja (2024), *Il quadro normativo UE sull'Intelligenza Artificiale: gli aspetti innovativi del nuovo regolamento*, in "De Iustitia", n. 3, 2024

G. Baum (2023), *La commedia ai tempi di ChatGPT. Ovvero, ecco perché l'IA non è divertente (almeno per ora)*, in "The Hollywood Reporter", 6 giugno 2023

G. Bender (2023), *The global AI race – it's time to slow down*, in "Social Europe", 15 February 2023

J.R. Biden (2023), *Safe, Secure and Trustworthy Development and Use of Artificial Intelligence*, Executive Order 14110 of October 30, 2023

E. Bocchini (2024), *La regolazione giuridica dell'intelligenza artificiale*, Giappichelli, 2024

S. Bonavita, A. Cortina (2024), *L'AI Act a rischio corto circuito: ecco i problemi nell'applicazione pratica*, in "Agenda digitale", 2 ottobre 2024

73. Sui rischi che i sistemi di IA possono presentare nei confronti dei diritti fondamentali e sulla conseguente necessità di elaborare "protezioni etiche" ("*ethical guardrails*") a livello mondiale si veda: United Nations Educational, Scientific and Cultural Organization – UNESCO, Recommendation on the Ethics of Artificial Intelligence: key facts, (adopted on 23 November 2021), 2023. Il messaggio introduttivo di Gabriela Ramos (Social and Human Sciences, UNESCO) è sul sito dell'UNESCO. Un'altra importante iniziativa promossa dall'UNESCO in questo campo è costituita dal Global AI Ethics and Governance Observatory, Osservatorio realizzato con l'obiettivo di fornire una risorsa globale ai decisori politici, ma anche agli accademici, al settore privato e alla società civile in genere, al fine di elaborare soluzioni alle sfide più urgenti sollevate dall'Intelligenza artificiale. L'Osservatorio ospita, a sua volta, l'AI Ethics and Governance Lab, che raccoglie documentazione relativa a casi di studio, buone pratiche e ricerche di punta, in modo da fornire un supporto concreto e strumenti innovativi per un adeguato inquadramento delle principali problematiche connesse all'IA.

A. Burt (2021), *New AI Regulations Are Coming. Is Your Organization Ready?*, in "Harvard Business Review", April 30, 2021

L. Camaioni (2016), *La Teoria della mente. Origini, sviluppo e patologia*, Fabbri, 2016

A. Capacci, G. Galli, A. Loreggia, I. Maroccia (2024), *Il nuovo regolamento europeo sull'IA: cosa cerca di fare e cosa fa*, in "Osservatorio CPI, Conti Pubblici Italiani", 22 febbraio 2024

M. Castigli, P. Sandonnini (2024), *ChatGPT guida completa: cos'è, come si usa e cosa può fare per aziende e professionisti*, in "Agenda digitale", 25 ottobre 2024

C. Cath, S. Watcher, B. Mittelstadt et al. (2018), *Artificial intelligence and the "Good Society": the US, EU and UK approach*, in "Science and Engineering Ethics", vol. 24, 2018

A. Cavazzuti (2024), *Provider e Deployer nell'AI Act: chi sono e cosa fanno?*, in "Studio legale Delli Ponti", 16 aprile 2024

E. Chiti, B. Marchetti (2020), *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in "Rivista della regolazione dei mercati", 2020, n. 1

S. Chudleigh (2024), *Che cos'è un agente AI*, in "botpress", 31 maggio 2024

E. Cirone (2024), *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in "Quaderni AISDUE", n. 2/2024, fascicolo speciale su "La nuova disciplina UE sull'intelligenza artificiale"

Commissione europea (2021), *Piano coordinato sull'intelligenza artificiale*, 2021

Commissione europea (2020), *Un nuovo piano d'azione per l'economia circolare. Per un'Europa più pulita e più competitiva*, COM(2020) 98, 11 marzo 2020

Consiglio di Stato cinese (2017), *New Generation Artificial Intelligence Development Plan – AIDP* (trad. a cura di G. Webster, R. Creemers, E. Kania, P. Triolo), in "DigiChina", Stanford University, August 1, 2017

Consiglio europeo, Consiglio dell'Unione europea (2024), *In che modo l'UE rafforza la propria cibersicurezza*, 2 dicembre 2024

G. Coraggio (2024), *Siete un Provider o un Deployer ai sensi dell'AI Act?*, in "Diritto al digitale", 2 aprile 2024

Corte dei conti europea (2024), *Intelligenza artificiale: l'UE deve accelerare il passo*, 29 maggio 2024

M. D'Ascenzo (2024), *Venture capital, in Europa i fondi puntano sull'intelligenza artificiale*, in "Il Sole 24 ore", 18 ottobre 2024

T. De Bree (2024), *La scomoda verità della normativa europea sull'intelligenza artificiale (AI Act)*, in "Risk & Compliance", 5 gennaio 2024

M. De Leo, B. Biscaretti di Ruffia (2024), *La responsabilità del deployer nell'uso dell'Intelligenza Artificiale*, in "DB - Non solo diritto bancario", 17 dicembre 2024

M. Do Couto (2024), *Entering the Age of Explainable AI*, in "TDWI – Transforming Data With Intelligence", 2024

Douglas Heaven (2017), *The epic robot fails that say ai will never rule the world. Will the machines rise up and enslave us? The history of incompetent robots, from klutzy cleaners to sense-mangling chatbots, suggests we can sleep easy*, in "New Scientist", 19 December 2017

E. Dusi (2024), *Il Premio Nobel per la Fisica a John Hopfield e Geoffrey Hinton per l'intelligenza artificiale*, in "La Repubblica", 8 ottobre 2024

F. Faggin (2024), *Oltre l'invisibile. Dove scienza e spiritualità si uniscono*, Mondadori, 2024

F. Faggin (2022), *Irriducibile. La coscienza, la vita, i computer e la nostra natura*, Mondadori, 2022

A. Fawzi, B. Romera-Paredes (2023), *FunSearch: Making new discoveries in mathematical sciences using Large Language Models*, in "Google DeepMind", 14 December 2023

E. Fleischner (2023), *Perché non bisogna avere paura dell'Intelligenza Artificiale, ma solo fare attenzione*, in "Spirito Artigiano", 16 settembre 2023

Garante per la Protezione dei Dati Personali (2021), *Assistenti digitali (smart assistant): i consigli del Garante per un uso a prova di privacy, Scheda informativa*, marzo 2021

A. Glushenkov (2024), *Deep Blue: The Chess Supercomputer That Changed AI and IBM Forever*, in "Medium", November 2, 2024

A. Gui, P. Ivankovich, S. Mancini et al. (2024), *AI Act, come definire ruoli e responsabilità per evitare sanzioni: la guida per imprese e P.A.*, in "Agenda digitale", 4 novembre 2024

F. Hsu (2004), *Behind Deep Blue: Building the Computer That Defeated the World Chess Champion*, Princeton University Press, 2004

M. Iaselli (a cura di) (2024), *AI Act. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli editore, 2024

IBM (Red.) (2020), *Che cos'è l'AI spiegabile (XAI)*, 2020

E. Intini (2024), *Geoffrey Hinton, quella volta che il Nobel "padrino pentito dell'AI" lasciò Google*, in "Focus", 8 ottobre 2024

E. Intini (2017), *Hawking: Il nostro tempo come specie dominante sulla Terra sta per scadere*, in "Focus", 9 novembre 2017

S. Khanal, H. Zhang, A Taeihagh (2024), *Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities*, in "Journal of Contemporary China", 9 April 2024

V. Lalli (2024), *AI Act: approvato il testo del Regolamento UE sulla Intelligenza Artificiale*, in "Avvocloud.net. La rete di avvocati online", 29 settembre 2024

J. Landgrebe, B. Smith (2022), *Why Machines Will Never Rule the World. Artificial Intelligence without Fear*, Routledge, 2022

S. Lecce, E. Cavallini, A. Pagnin (2010), *La teoria della mente nell'arco di vita*, il Mulino, 2010

L. Longo, M. Brcic, F. Cabitza et al. (2024), *Explainable Artificial Intelligence (XAI) 2.0: A Manifest of Open Challenges and Interdisciplinary Research Directions*, in "Information Fusion", vol. 106, June 2024

J. Ma (2024), *The U.S. reigns supreme in A.I. startups while China ensures chatbots have 'core socialist values'*, in "Fortune", July 21, 2024

S. Maggiolo (2016), *L'intelligenza di AlphaGo*, in "Il Post", 21 marzo 2016

B. Marr (2024), *7 Ways To Turn The "Bring Your Own AI" Threat Into An Opportunity*, in "Forbes", August 22, 2024

A.A. Martino (2024), *Dove sta andando l'intelligenza artificiale?*, in "Il Sole 24 ore. NT+Diritto", 4 ottobre 2024

A. McAfee, E. Brynjolfsson (2016), *Where Computers Defeat Humans and Where They Can't*, in "The New York Times", March 16, 2016

S. Mele (2025), *Rischi e opportunità dell'AI Act in attesa del Vertice di Parigi*, in "Formiche", 8 febbraio 2025

R. Metz (2018), *Microsoft's neo-Nazi sexbot was a great lesson for makers of AI assistants*, in "MIT Technology Review", March 27, 2018

M. Mialich (2021), *Smart Assistant: profili di criticità e raccomandazioni delle Autorità per la protezione dei dati personali*, in "CyberLaws", 21 giugno 2021

J. Mouret (2024), *Large Language Models help computer programs to evolve*, in "Nature", 17 January 2024

E. Musk et al. (2017), *An Open Letter to the United Nations Convention on Certain Conventional Weapons*, Future of Life Institute, 20 August, 2017

New Scientist (2018), *Machines that Think. Everything you need to know about the coming age of artificial intelligence* (trad. it. V.L. Gili, "Macchine che pensano. La nuova era dell'Intelligenza Artificiale", Edizioni Dedalo, dicembre 2018)

R. Panetta (2024), *AI Act: critiche sbagliate, era urgente regolare l'Intelligenza Artificiale*, in "Agenda digitale", 26 marzo 2024

Parlamento europeo (2023), *Economia circolare: definizione, importanza e vantaggi*, 25 maggio 2023

M. Pedrazzoli (2024), *La Corte dei conti UE lancia l'allarme: nell'Unione non si sta facendo abbastanza per sviluppare l'Intelligenza artificiale*, in "EU News", 29 maggio 2024

M. Polanyi (1966/1979), *The Tacit Dimension*, 1966 (trad. it. "La conoscenza inespressa", Armando Editore, 1979)

M. Polanyi (1958/1990), *Personal Knowledge: Towards a Post-Critical Philosophy*, 1958 (tr. it. "La conoscenza personale", Rusconi, 1990)

C. Ponti (2024), *AI Act, sacrificati i diritti dei più deboli: ecco perché*, in "Cybersecurity 360", 15 marzo 2024

A.Z. Ren, A. Dixit, A. Bodrova et al. (2023), *Robots That Ask For Help: Uncertainty Alignment for Large Language Model Planners*, in "arXiv", 4 September 2023

La Repubblica (Red.) (2025), *Lee SeDol giocava a Go come un Dio. Ma da quando una IA l'ha battuto, non è più lo stesso*, 16 luglio 2024 (aggiornato 20 febbraio 2025)

La Repubblica (Red.) (2016), *Microsoft, il chat-bot Tay scrive frasi razziste: cancellati i suoi tweet*, 25 marzo 2016

H. Roberts, J. Cowls, J. Morley et al. (2021), *The Chinese Approach to AI: An Analysis of Policy, Ethics, and Regulation*, in "AI and Society", vol. 36, 2021, n. 1

B. Romera-Paredes, M. Barekatain, A. Novikov et al. (2024), *Mathematical discoveries from program search with large language models*, in "Nature", vol. 625, 2024

M. Rovelli, P. Ottolina (2024), *Chi è Geoffrey Hinton, «padrino» pentito dell'intelligenza artificiale, che ha vinto il Nobel: «È spaventosa»*, in "Corriere della sera", 8 ottobre 2024

P. Sandonnini (2024), *AI Act in vigore dal 1° agosto, ma già piovono critiche. E l'Ue si difende*, in "AI4Business", 16 luglio 2024

C. Shannon (1950), *Programming a Computer for Playing Chess*, in "Philosophical Magazine", vol. 41, 1950, n. 314

D. Silver, A. Huang, C.J. Maddison et al. (2016), *Mastering the Game of Go with Deep Neural Networks and Tree Search*, in "Nature", vol. 529, 27 January 2016

P. Speroni di Fenizio (2024), *L'Eu AI Act e i suoi problemi*, in "Futura Network", 11 luglio 2024

S. Stefanelli, A. Terrizzi (2024), *AI Act e responsabilità penale, cosa cambia per provider e deployer*, in "Agenda digitale", 17 luglio 2024

Studio Gartner (2024), *Le 10 principali tendenze tecnologiche strategiche per il 2025*, in "AI4Business", 22 ottobre 2024

S. Sulmicelli (2023), *Stati Uniti d'America – Executive Order on The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, in "BioDiritto", 30 ottobre 2023

U.S. Department of Commerce, Office of Public Affairs (2024), *U.S. and UK Announce Partnership on Science of AI Safety*, April 1, 2024

N. van der Meulen, B. H Wixom (2024), *Bring Your Own AI: How to Balance Risks and Innovation*, in "MIT Sloan Management Review", October 3, 2024

A. Viliotti (2024), *Agenti AI: Intelligenza Artificiale per il pensiero, l'organizzazione e l'impiego di strumenti*, 29 aprile 2024

A. Viliotti (2023), *Scopri come KnowNo sta cambiando il futuro della robotica*, in "Linkedin", 13 dicembre 2023

P. Voigt, N. Hullen (2024), *The EU AI Act: Answers to Frequently Asked Questions*, Springer, 2024

B. Vranken (2023), *Big Tech lobbying is derailing the AI Act*, in "Corporate Europe Observatory", 24 November 2023

M.J. Wolf, K.W. Miller, F.S. Grodzinsky (2017), *Why We Should Have Seen That Coming. Comments on Microsoft's Tay "Experiment", and Wider Implications*, in "The ORBIT Journal", vol. 1, 2017, n. 2

T. Zia (2024), *Agentic AI: come i grandi modelli linguistici stanno plasmando il futuro degli agenti autonomi*, in "Unite.AI", 1° novembre 2024

L. Zorloni (2024), *Inizia la stagione dell'AI Act: ecco le 6 scadenze del Regolamento europeo sull'Intelligenza artificiale*, in "Wired", 12 luglio 2024

R. Zreick (2018), *Perché non devi avere paura dell'Intelligenza Artificiale*, in "Focus", 21 gennaio 2018

V. Zucconi (1997), *Kasparov – Deep Blue, sfida truccata*, in "la Repubblica", 8 maggio 1997

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0223 • articolo sottoposto a peer review • pubblicato in anteprima il 10 lug. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Chiara Spiniello

È (ancora) tempo di costituzionalismo digitale

Gli straordinari scenari di progresso – e, parallelamente, le nuove forme di potere e soggezione – che l'affermazione delle tecnologie "cyber-digitali" porta con sé hanno spinto l'Unione europea a intraprendere un percorso originale nella governance di Internet volto a combinare i principi del costituzionalismo digitale con le aspirazioni in ordine alla sovranità digitale. Il contributo, dopo aver definito il concetto di costituzionalismo digitale, ne analizza la conformazione assunta – in primo luogo – nel dibattito e negli atti legislativi europei. Successivamente, effettuando un'indagine qualitativa di stampo comparativo, prende in esame le politiche nazionali digitali e i discorsi politici di tre Stati membri (Francia, Germania, Italia), selezionati per la peculiare posizione assunta sul tema. Le conclusioni, evidenziando l'emersione di interessi nazionali confliggenti col progetto europeo che rischiano di comprometterne il delicato equilibrio, portano ad interrogarsi sull'attualità e sull'attuabilità degli assi portanti del costituzionalismo digitale.

Costituzionalismo digitale – Sovranità digitale – Internet governance – Unione europea – Politiche digitali nazionali

The time for digital constitutionalism is (still) now

The remarkable prospects for progress — alongside emerging forms of power and subjugation — associated with the rise of cyber-digital technologies have prompted the European Union to pursue a distinctive approach to Internet governance, seeking to reconcile digital constitutionalism with ambitions for digital sovereignty. This contribution first defines the notion of digital constitutionalism and examines its development within European legal and political discourse. It then undertakes a qualitative, comparative analysis of national digital strategies and political narratives in three Member States (France, Germany, and Italy), selected for their distinctive stances. The conclusions underline how conflicting national interests risk undermining the fragile balance of the European project, casting doubt on the viability and contemporary relevance of digital constitutionalism's foundational principles.

Digital constitutionalism – Digital sovereignty – Internet governance – European Union – National digital policies

L'Autrice è assegnista di ricerca presso l'*Internet and Communication Policy Center* (ICPC), Dipartimento di Scienze Aziendali – Management & Innovation Systems (DISA–MIS), Università degli Studi di Salerno

Il presente contributo è uno dei risultati delle attività di ricerca svolte nell'ambito del progetto PRIN 2022KTTSBC – Digital Sovereignty in Comparative Perspective: State Authority, Corporate Power and Fundamental Rights in Cyberspace (CUP Master D53D23007300006)

Sommario: 1. Costituzionalismo digitale: cosa, quando e (soprattutto) perché. – 2. La "terza via" dell'Unione europea: tra costituzionalismo e sovranità digitale. – 3. La prospettiva degli Stati membri: uno sguardo comparato. – 3.1. Francia: *souveraineté, marché, sécurité*. – 3.2. Germania: *für eine kollektive und individuelle (wirtschaftliche) digitale Souveränität*. – 3.3. Italia: la "Agenda Digitale Mattarella". – 4. Sovranità digitale *versus* costituzionalismo digitale. – 5. Costituzionalismo digitale: suona già come un anacronismo?

1. Costituzionalismo digitale: cosa, quando e (soprattutto) perché

Quindici anni sono ormai trascorsi da quando, nell'autunno del 2010, Stefano Rodotà teorizzava la sua "Costituzione per Internet"[1], una *Costituzione infinita*, discendente non già dall'applicazione di una dimensione verticale del potere con norme sovrastatali incorporate nei diritti statali o in esso traslate; bensì frutto di "una costruzione del diritto per espansione, orizzontale", in quanto risultante da "un insieme di ordini giuridici correlati"[2].

Dunque, non una Costituzione *subita*, quanto piuttosto una globalmente condivisa, derivante da un processo deliberativo *multi-stakeholder*, con protagonisti gli esponenti governativi, ma anche i rappresentanti del settore privato e della società civile.

Soprattutto, una Carta che si occupasse di disciplinare la tutela dei diritti fondamentali degli individui nella rete e che, al contempo, si preoccupasse di limitare (e di ridistribuire) l'esercizio del potere nello spazio digitale: quelli che insomma sono, al netto della qualificazione "digitale", gli scopi "classici" della teoria costituzionale[3]. Infatti, se dapprincipio – nella seconda metà del Settecento – come conseguenza delle Rivoluzioni americana e francese, l'obiettivo del costituzionalismo era quello di circoscrivere il potere del Sovrano e successivamente, con l'emanazione dei testi costituzionali c.d. "rigidi", di razionalizzare l'autorità dello Stato, oggi la sua più grande sfida (una delle) è rappresentata dalle nuove tecnologie, o, più esattamente, dalla salvaguardia dei diritti di libertà dell'individuo di fronte alle implicazioni derivanti dal mondo digitale con le logiche di potere che lo governano. E si trova a farlo, il costituzionalismo, confrontandosi con paradigmi del tutto rinnovati rispetto al passato: non vi è più solo un potere (privato o pubblico)[4] da fronteggiare, non più uno spazio delimitato[5] da tutelare. A dominare la nuova società digitale – che non ha confini territoriali – non è, infatti, la (sola) autorità statuale, gli *stanchi* vecchi *giganti di carne*

1. Cfr. Rodotà 2010.
2. *Ivi*, p. 351.
3. Sulla nozione di "costituzionalismo" si vedano, tra gli altri, Frosini 2019; Barber 2018; Grimm 2018; Sajó 1999; Mirkine-Guetzévitch 1933. Ha effettuato una disamina esaustiva delle diverse accezioni attribuite al termine Celeste 2020.
4. Cfr. Cavani 2023, p. 224.
5. Storicamente maturati nel contesto dello Stato, i valori del costituzionalismo negli ultimi decenni sono stati chiamati a riadattarsi ad una società sempre più globale, in cui la centralità dell'istituzione statale è svanita a causa dell'emergere di altri attori dominanti nel contesto transnazionale. Il mito del legame obbligatorio tra costituzionalismo e Stato è così stato sfatato. Cfr. Preuss 2010.

e acciaio[6], ma sono (anche e ancor di più) poteri privati che agiscono "con forme di cogenza e autorità pubbliche"[7], i nuovi *giganti del web*[8]. Il binomio "diritto-tecnologia", da sempre esistito nella storia dell'evoluzione umana[9], diviene così parte di una nuova relazione, questa volta trinomia: "diritto-tecnologia-poteri privati", la cui definizione è tutta in divenire.

È evidente, l'influenza esercitata dalle nuove tecnologie sulle nostre vite è stata, sin dalla loro primigenia comparsa, significativa; tuttavia, negli ultimi decenni le tecnologie "cyber-digitali" hanno affermato sé stesse come orizzonte indispensabile e imprescindibile per l'esistenza umana, con le evidenti contraddizioni che ne derivano. Se per un verso, infatti, l'avvento e la diffusione di Internet e della rete hanno aperto straordinari scenari di progresso – anche in termini di espressione e godimento dei diritti fondamentali, prima fra tutte la libertà di manifestazione del pensiero, "pietra angolare dell'ordine democratico"[10] –; per altro verso, gli stessi hanno originato delle nuove forme di soggezione, dinnanzi alle quali le minacce alle prerogative costituzionali poste a tutela dell'individuo si sono fatte più gravi e pericolose[11]. Se a ciò si aggiunge, poi, che il potere pubblico (o, meglio, il suo abuso) non è più l'unico motivo di apprensione in relazione al rispetto dei diritti fondamentali e alla salvaguardia della democrazia[12], si comprende bene come l'esercizio di definizione e bilanciamento che storicamente il costituzionalismo è chiamato ad assolvere si arricchisce, oggi, di significati e sfide, a tal punto inedite da far parlare di un nuovo "momento costituzionale"[13].

Una fase *in itinere* e alla cui definizione in molti hanno tentato e stanno tentando di contribuire.

6. Così John Perry Barlow definiva i "Governi del mondo industriale" in Barlow 1996.
7. Così Lombardi 1970, p. 45. Il tema del rapporto tra poteri pubblici e privati non è certamente nuovo alla riflessione giuridica, si citano qui due grandi classici, rispettivamente della dottrina giusprivatista e costituzionalista, Esposito 2003 e Bianca 1977.
8. L'espressione è presa in prestito da Armando Lamberti che così definisce le grandi piattaforme digitali. Cfr. Lamberti 2023. A proposito della commistione tra poteri pubblici e privati nell'era digitale, Celeste 2021, pp. 105-118, argomenta che: "attraverso sofisticate tecnologie, gli Stati sono oggi in grado di monitorare in generale la vita di milioni di cittadini, interferendo significativamente in aspetti della loro vita privata. Allo stesso tempo, la natura globale dello spazio virtuale ha favorito l'emergere di società private multinazionali come nuovi attori dominanti affianco agli Stati nazione".
9. Sul punto Costanzo 2014.
10. Secondo la celebre definizione proposta dalla Corte costituzionale nella sentenza n. 84 del 1969, orientamento confermato altresì nella sentenza n. 126 del 1985, dove definisce la libertà di manifestazione del pensiero "cardine di democrazia nell'ordinamento generale". In senso analogo, anche le sentenze: n. 11 del 1968, in cui il diritto di cui all'art. 21 Cost. è ritenuto "coessenziale al regime di libertà garantito dalla Costituzione"; n. 98 del 1968, secondo cui la "libertà di manifestazione del pensiero […] è ordine dell'ordinamento democratico"; n. 126 del 1985 (già citata), ove si ribadisce "la rilevanza centrale […] che la libertà di manifestazione del pensiero, anche e soprattutto in forma collettiva, assume ai fini dell'attuazione del principio democratico". È fin troppo semplice riportare degli esempi di come la rete abbia ampliato la portata di tale diritto: l'implementazione delle piattaforme digitali ha rappresentato un canale straordinario per diffondere le proprie convinzioni politiche o religiose, nonché per organizzare momenti assembleari e di protesta.
11. Come fa notare Celeste 2021, p. 107 "diffamazione, disinformazione, bullismo, molestie, incitamento all'odio non rappresentano nuovi pericoli del ventunesimo secolo [ma la loro] *variante* online" e, quindi, aggiungo io, il loro potenziale di diffusione su ampissima scala, ha aumentato esponenzialmente il numero (e le modalità) di violazione dei diritti che ledono.
12. Si pensi, in tal senso, alla funzione di vigilanza rispetto alla produzione, diffusione e controllo del flusso informativo messa in atto dalle grandi piattaforme digitali, le quali – in tal modo – hanno preso ad esercitare un potere censorio, privato, che mal si adatta ai principi fondanti dello Stato costituzionale di diritto. Per un approfondimento sul tema si rimanda, tra gli altri, a Vasino 2023; Monti 2019; Gillespie 2018.
13. Così Celeste 2018, p. 3.

Quella di Rodotà, alla cui riflessione in tema di diritto e tecnologia molto dobbiamo[14], invero non è stata l'unica proposta di regolamentazione costituzionale della rete. Numerose sono state, infatti, le teorizzazioni in materia e diversi i concreti tentativi susseguitesi dagli inizi del nuovo millennio, quando divenne ormai chiaro che il mito del cyberspazio capace di autoregolarsi e, dunque, naturalmente indipendente e non soggetto alla tirannia e alla *sovranità* statale – così come descritto da John Perry Barlow nella sua *Declaration of the Independence of Cyberspace* – null'altro era che, per l'appunto, un mito[15].

Sotto il profilo teorico, è impossibile esimersi dal citare, innanzitutto, lo scritto *Code and Other Laws of Cyberspace* di Lawrence Lessig, considerato un "classico degli studi giuridici e politici sulla rete"[16], in cui il *codice* – ossia la stessa architettura di Internet – *è* la *legge*, legge in azione, e, dunque, potenzialmente Costituzione in azione. Mi spiego: a detta di Lessing il complesso delle strutture materiali e immateriali che formano e definiscono la struttura del cyberspazio funge, esso stesso, da meccanismo di regolamentazione della rete. Tale architettura, chiarisce il Nostro, non può continuare ad essere plasmata esclusivamente dalle aziende tecnologiche, mosse da interessi puramente economici, ma deve incorporare i principi costituzionali, in particolare quelli sanciti dalla Costituzione americana, che le consentano di agire in difesa dei diritti fondamentali degli utenti[17].

Si discosta invece dall'idea di una trasposizione diretta di principi già esistenti, la prospettiva del *costituzionalismo sociale* delineata dal giurista tedesco Gunther Teubner, secondo il quale – in considerazione della natura composita e transnazionale della società digitale – i classici processi politici di costituzionalizzazione non sono idonei a delineare la Costituzione della rete, che può di contro originare esclusivamente da un processo sociale. Sono, cioè, quelli che Teubner definisce i "settori spontanei della società" (agenzie governative, gruppi della società civile, sindacati, ecc.) ad avere il compito di emanare in autonomia norme costituzionali, assorbite dal sistema giuridico e da esso armonizzate, le quali concorrono a realizzare una "moltitudine di Costituzioni civili" della rete[18].

Lo spunto di una pluralità di Carte civili per il digitale, d'altra parte, è ripreso anche dal costituzionalista Gaetano Azzariti che, pur individuando nel carattere della globalità la più efficace risposta in relazione alla tutela dei diritti fondamentali in Internet, mette in guardia sul fatto che un unico documento universalmente valido possa originare una forma di "colonialismo costituzionale" e che, pertanto, sono da preferire più Carte e dichiarazioni, elaborate da vari attori, compresa la società civile[19]. Rivaluta, invece, la soluzione di una forma di costituzionalismo globale multilivello Ingolf Pernice, studioso di *Global Constitutionalism*, che immagina una costruzione complessa in cui tutti i sistemi giuridici parziali si completano a vicenda per dare forma a un "quadro costituzionale globale", in cui il costituzionalismo statale non è assente ma agisce in sincrono con gli attori privati, che detengono un fondamentale ruolo di co-regolazione[20].

Ciò detto, e come anticipato, l'idea di una Carta scritta dei diritti di Internet non è rimasta un prototipo teorico, una "mera" astrazione accademica, trovando una sua traduzione pratica nella proposizione di diversi *Internet Bill of Rights* da parte sia di gruppi costituitisi in seno alla società civile sia di organizzazioni e istituzioni politiche. Tutti testi che, pur giuridicamente non vincolanti perché sprovvisti di un sistema sanzionatorio e di efficaci meccanismi di attuazione, sono nati con l'obiettivo di promuovere un modello di trasformazione digitale fondato sulla centralità della persona umana,

14. Come pure lo ricorda Azzariti 2022. Tra gli scritti di Stefano Rodotà in argomento si ricordano, accanto al già citato *Una Costituzione per Internet?*, Rodotà 1997, Rodotà 2012, Rodotà 2014.
15. In controtendenza, continua a sostenere siffatta visione Mueller 2020, pp. 779-801.
16. Cfr. Amoretti–Santaniello 2024, p. 33.
17. Cfr. Lessig 1999; successivamente riedito, Lessig 2006.
18. Cfr. Teubner 2004; nonché Teubner 2012.
19. Cfr. Azzariti 2011, pp. 367-378.
20. Cfr. Pernice 2016.

nel rispetto di valori e principi universalmente condivisi.

Dal *Marco Civil da Internet* brasiliano, il primo statuto approvato nel 2014 da un Parlamento nazionale contenente "principi, garanzie, diritti e obblighi per l'uso di Internet", alla *Dichiarazione africana sui diritti e le libertà di Internet* pubblicata, in quello stesso anno, dall'*African Declaration Group*; dal *Code of Ethics for the Information Society*, adottato dall'UNESCO nel 2011, alla *Dichiarazione dei diritti in Internet* redatta nel 2015 da una commissione composta da politici, accademici, rappresentanti di aziende private e ONG e presieduta da Stefano Rodotà.

A sintetizzare questa "costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di governance, e limitazioni all'esercizio del potere su Internet"[21] è intervenuto il *Berkman Center for Internet and Society* dell'Università di Harvard coniando l'espressione *digital constitutionalism*[22].

Ebbene, questo è il costituzionalismo digitale. Perché ne abbiamo bisogno? Facile a dirsi: un tempo c'era un Re, subito dopo lo Stato, oggi dei *CyberSovrani.* Contro i quali difendersi.

2. La "terza via" dell'Unione europea: tra costituzionalismo e sovranità digitale

Più di tutti, disegnando una "terza via nella *governance* globale di Internet"[23], è stata l'Unione europea a intraprendere un percorso di progressiva regolamentazione dell'ecosistema digitale.

Dapprincipio, lo ha fatto mediante la diffusione di atti di *soft law*[24], come le Raccomandazioni del Parlamento (risale a più di quindici anni fa, ad esempio, la Raccomandazione relativa al "Rafforzamento della sicurezza e delle libertà fondamentali su Internet" del 26 marzo 2009[25]), le Dichiarazioni del Consiglio (le più recenti "Dichiarazione sull'e-Government" del 6 ottobre 2017, "Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori" dell'8 dicembre 2020, "Dichiarazione di Lisbona – Democrazia digitale con uno scopo", del 1° giugno 2021[26]), le strategie politiche della Commissione (come quella "per il mercato unico digitale in Europa" del 6 maggio 2015[27]), o infine gli atti adottati congiuntamente dalle tre Istituzioni, tra cui si ricorda la recente "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" datata 23 gennaio 2023[28].

21. Cfr. Gill–Redeker–Gasser 2015, p. 2.
22. Tale definizione è stata proposta nel Report di ricerca succitato, nel quale gli Autori hanno passato in rassegna 30 documenti, pubblicati tra 1999 e il 2015, effettuando un'analisi lessicale, sia qualitativa che quantitativa, del concetto di *digital constitutionalism*. Interessante è anche lo studio effettuato da Santaniello–Palladino–Catone–Diana 2018, pp. 320-333, sulle proposte effettuate dai Parlamenti nazionali sul tema.
23. "Alternativa tanto al modello di *private self-regulation* promosso dagli USA quanto al modello stato-centrico a guida governativa sostenuto dai regimi autoritari". Cfr. Santaniello 2022, p. 50. Come si avrà modo di dire più avanti, da una parte, gli Stati Uniti – grazie alla copertura del Primo Emendamento in tema di *free speech* e mediante la *Section 230* del *Communications Decency Act* emanata dal Congresso nel 1996 – hanno predisposto un quadro normativo fortemente protettivo per le imprese che operano nella sfera digitale, realizzando un'ampia delega del potere di autoregolamentazione ai privati e, di contro, limitando notevolmente il potere regolatorio degli enti statali; dall'altra parte, la Cina e la Russia – considerando Internet, il web e le piattaforme digitali come infrastrutture tecniche fondamentali, elemento essenziale di una strategia nazionale unitaria – hanno messo in piazza un sistema di governo incentrato sulla centralità dello Stato nella definizione delle regole del *gioco digitale*.
24. La letteratura in tema di *soft law* è piuttosto ampia. Si richiamano qui, per le nozioni di base, Mostacci 2008; Somma 2008, p. 437 ss.; Pastore 2003, pp. 5-16.
25. Cfr. European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)).
26. L'insieme delle Dichiarazioni è consultabile nel sito web ufficiale del Consiglio.
27. I contenuti del documento sono rinvenibili alla pagina *Dipartimento per gli Affari Europei – Strategia per il mercato unico digitale*.
28. Cfr. European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01).

Successivamente, sotto la spinta della giurisprudenza delle Corti europee, in specie le sentenze della Corte di giustizia dell'Unione europea, tramite l'emanazione di atti aventi la cogenza della legge. Prima di passare in rassegna questi ultimi, ha senso riflettere proprio sull'operato della CGUE e, in particolare, su quanto i suoi giudizi abbiano assunto un valore prescrittivo e, non meno importante, in quale misura essi abbiano influito sulla decisione del legislatore europeo di (ri)appropriarsi del suo ruolo di *lawmaker* in ambito digitale[29].

Storicamente la Corte di giustizia europea ha ricoperto un ruolo fondamentale per l'acquisizione di una posizione di centralità nell'ordinamento dell'Unione da parte dei diritti fondamentali; ruolo che si è confermato di primaria importanza nella materia dell'*Internet governance*, dal momento che l'apporto della Corte è stato decisivo per l'operatività in ambito digitale dei valori e dei principi sanciti dai Trattati e dalle Carte europee[30]. Nella sua attività di interpretazione creativa la CGUE ha, infatti, attribuito a disposizioni pensate per operare in un ambiente analogico e, secondo alcuni Autori, talvolta "in aperto contrasto con il tenore letterale" delle stesse[31], una portata ben più ampia, suscettibile di produrre effetti orizzontali diretti nei confronti di soggetti privati, rispetto a quella che era stata loro attribuita *ab origine*. Paradigmatica è l'interpretazione proposta per gli artt. 7 e 8 della Carta dei diritti fondamentali, che tutelano, rispettivamente, la vita privata e i dati personali. In una corposa giurisprudenza emanata tra il 2014 e il 2015 (nell'ambito della quale rientrano le emblematiche sentenze C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González,* 2014; C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.,* 2014; C-362/14, *Maximillian Schrems c. Data Protection Commissioner,* 2015)[32], la Corte di giustizia dell'Ue, assumendo come base del proprio ragionamento i contenuti della direttiva 95/46/CE[33], ha affermato il principio della tutela della privacy digitale nei confronti della posizione di (sempre maggior) potere assunta dagli algoritmi, dall'intelligenza artificiale e dai motori di ricerca in generale. Nello specifico, nella sentenza *Google Spain*, la CGUE – considerando i motori di ricerca, come *Google*, responsabili del trattamento dei dati personali e ritenendoli quindi soggetti agli obblighi della direttiva in oggetto – ha riconosciuto agli utenti la possibilità di rivolgersi agli stessi motori di ricerca per ottenere la rimozione degli indici di informazioni personali obsolete, irrilevanti o infondate sancendo così il "diritto alla deindicizzazione" (o "diritto all'oblio")[34]. Nell'ambito della pronuncia *Digital Rights Ireland*, poi, la Corte ha dichiarato

29. Una simile riflessione, in effetti, andrebbe estesa anche ai livelli nazionali di governo, dove le Alte Corti – nella loro attività interpretativa creativa – negli ultimi decenni si sono mostrate decisamente attive nei silenzi del legislatore. La letteratura sul tema è sterminata, in questa sede non ci si può esimere dal citare un "classico" sui rapporti tra Corte e legislatore: Zagrebelsky 1981.
30. Sui principali profili di distinzione giuridica tra diritti fondamentali e valori si veda, in particolare, Baratta 2019; Cannizzaro 2018.
31. Così Pollicino 2023, p. 579; si veda anche Pollicino 2018, pp. 138-163.
32. Accanto a queste, tra le sentenze della Corte di giustizia riguardanti il trattamento di dati personali, si ricordano: Corte di giustizia, sentenza del 17 luglio 2014, cause riunite C-141/12 e C-372/12, *Y.S. e a.*; Corte di giustizia, sentenza del 2 ottobre 2014, causa C-127/13 P, *Strack/Commissione*; Corte di giustizia, sentenza dell'11 dicembre 2014, causa C-212/13, *Ryneš*; Corte di giustizia, sentenza del 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a.*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-615/13 P, *ClientEarth e PAN Europe/EFSA*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-580/13, *Coty Germany*; Corte di giustizia, sentenza del 1° ottobre 2015, causa C-201/14, *Bara e a.*; Corte di giustizia, sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo*.
33. Cfr. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
34. Tale decisione rappresenta non solo un passaggio fondamentale per il riconoscimento del diritto all'oblio, ma – secondo alcuni Autori – anche un caso emblematico di gestione "privatizzata" dei diritti fondamentali. La Corte, infatti, affida interamente ai motori di ricerca il compito di equilibrare l'interesse collettivo alla diffusione

l'invalidità della direttiva 2006/24/CE sulla conservazione dei dati, giudicata viziata perché incidente in misura sproporzionata sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale così come predisposti dalla direttiva 95/46/CE e dalla Carta dei diritti fondamentali dell'Ue. Infine, con la decisione *Schrems I*, i giudici europei hanno invalidato il *Safe Harbor*, il regime atto a regolare il trasferimento di dati tra Ue e USA, ritenendolo non idoneo a garantire il principio della protezione dei dati personali sancito dall'art. 25 della direttiva 95/46/CE, secondo cui i dati personali possono essere trasferiti solo verso Paesi con un livello di protezione equivalente a quello europeo.

Al di là dell'ovvia considerazione sull'importanza strategica attribuita alla protezione dei dati personali online e alla volontà del giudice europeo di affermare con decisione il quadro delineato in materia nell'ambito dell'Ue, l'insieme di questa giurisprudenza mostra chiaramente come i *digital rights* abbiano per lungo tempo trovato una loro tutela esclusivamente a livello giurisdizionale, di fronte a un legislatore inizialmente inerme e poi sempre più in affanno. Ad una prima fase, intorno agli inizi del Duemila, caratterizzata dal dominio del liberismo digitale e dalla tutela incontrastata del principio di libera concorrenza di mercato, ne è seguita una seconda in cui le istituzioni europee – pur comprendendo la necessità di imbrigliare il crescente potere dei soggetti privati in rete – si sono trovate impreparate nel loro compito di normazione della sfera digitale, complice anche un dibattito politico particolarmente conflittuale.

In questo senso, le decisioni della CGUE hanno fornito un apporto significativo alla regolamentazione della materia, innanzitutto per quel che riguarda la protezione dei dati personali, contribuendo alla definizione del *General Data Protection Regulation* (GDPR), il Regolamento sul trattamento dei dati personali e la privacy approvato dal Parlamento europeo e dal Consiglio nel 2016 ed entrato in vigore nel 2018[35]. Tale atto ha, infatti, inaugurato una stagione di intensa attività legislativa delle istituzioni europee in materia digitale; stagione che, passando per l'emanazione dell'*Artificial Intelligence Act* (*AIA*), del *Cybersecurity Act* e del *Cyber Solidarity Act* (*CSA*) – rispettivamente atti a disciplinare gli ambiti dell'intelligenza artificiale e della sicurezza informatica –, è culminata, da ultimo, nell'adozione del *Digital Services Package* (DSP), composto dal *Digital Services Act* (DSA) e dal *Digital Markets Act* (DMA), contenente norme e principi volti ad assicurare argini più solidi ai poteri delle piattaforme online, con specifico riguardo alle attività di *content moderation*.

Ora, ad ispirare questa prolifica attività normativa[36] è stata certamente, e come detto, una rinnovata volontà da parte del legislatore europeo di salvaguardare i diritti fondamentali e di assicurare la tenuta dell'ordinamento democratico nell'ecosistema digitale, ma non solo. Si è, infatti, fatta strada negli orientamenti delle istituzioni dell'Ue il progetto della realizzazione di una *sovranità digitale* europea.

Impiegata per la prima volta in ambito europeo nei pareri del Comitato europeo delle Regioni e del Comitato economico e sociale europeo, la nozione di sovranità digitale è diventata ben presto d'uso comune nei discorsi dei leader politici e nei documenti ufficiali dell'Ue[37], fino ad approdare, di recente, nella dicitura "Technological Sovereignty, Security and Democracy" relativa agli ambiti di competenza della nuova vicepresidenza esecutiva,

delle informazioni con il diritto individuale alla loro rimozione. Un'operazione, ha ribattuto Oreste Pollicino, che "dovrebbe essere di esclusiva attribuzione di un'autorità giurisdizionale o para-giurisdizionale e la cui delega, quasi in bianco, a un operatore privato, senza le adeguate garanzie procedimentali […] non può fare altro che amplificarne il potere". Cfr. Pollicino 2023, p. 582. Per un'analisi di questa e delle altre sentenze in esame si vedano anche Amalfitano–Ferri 2024, pp. 1-34 nonché Finocchiaro 2015, pp. 779-799.

35. Per una disamina degli interventi normativi europei in tema di protezione dei dati personali si veda Spiniello 2018.

36. Secondo alcuni addirittura "ipertrofica". Sul punto Cfr. Pollicino 2023, p. 589.

37. Una ricostruzione dell'utilizzo del termine *digital sovereignty* in ambito europeo è stata effettuata da Alpini 2022, pp. 144-152.

costituita in seno alla Commissione von der Leyen II e attribuita a Henna Virkunnen[38]. Fortemente evocativa, la summenzionata locuzione consente di comprendere l'accezione che l'Unione europea ha dato ad un concetto, qual è quello di *digital sovereignty*, estremamente polisemantico[39]: nella costruzione europea, infatti, la sovranità tecnologica è posta in diretta correlazione con il tema della sicurezza e con i valori della democrazia.

In un contesto in cui il mercato dei prodotti e dei servizi digitali è dominato dalle multinazionali americane e cinesi, che conseguentemente impongono proprie regole e principi propri al funzionamento dello stesso, l'Unione europea pare aver sentito, forte, la necessità di porre un argine all'influenza delle (per non dire soggezione rispetto alle) aziende tecnologiche straniere. Muovendo dalla considerazione che il modello statunitense lascia un arbitrio incondizionato agli attori privati non sottoponendoli ad alcun tipo di controllo governativo, mentre quello cinese, antiteticamente, presuppone una supervisione governativa decisamente invasiva, l'Ue – per bocca della Commissione[40] – ha individuato nella risposta europea l'unica via percorribile perché capace di combinare lo sviluppo delle infrastrutture tecnologiche e la concorrenza tra gli attori economici con elevati *standard* di protezione dei diritti fondamentali in rete.

La *ratio* delle rivendicazioni di sovranità europee è, quindi, da individuarsi nella necessità di fronteggiare il rischio di un'eccessiva dipendenza rispetto ai Paesi non-Ue fornitori di servizi digitali, cosa che – oltre ad incidere sullo sviluppo economico dell'Unione – è suscettibile di esporre i cittadini Ue a potenziali violazioni dei diritti fondamentali, ai quali, peraltro, i *digital service provider* stranieri non è certo riescano a garantire un adeguato livello di protezione. L'Unione europea, invece, tramite gli investimenti nelle (e il controllo delle) infrastrutture digitali, ha l'ambizione di "mantenere inalterati i valori fondamentali di rispetto della democrazia e dei diritti umani di fronte alle sfide della società digitale globale"[41].

L'originalità del progetto digitale europeo, la famosa "terza via" cui si faceva cenno in apertura del paragrafo e poc'anzi ripresa, risiede proprio in questo: nel tentativo di combinare il concetto di costituzionalismo digitale con quello di sovranità digitale, in ottemperanza al principio secondo cui la progressione delle infrastrutture digitali europee deve avvenire sotto l'egida dei valori fondanti dell'Unione (solidarietà e inclusione, libertà di scelta, partecipazione, sicurezza in rete e sostenibilità, primi fra tutti).

3. La prospettiva degli Stati membri: uno sguardo comparato

Se gli assi portanti del discorso europeo su costituzionalismo e sovranità digitale sono tali, si può dire che i medesimi interessi muovano le politiche (e l'operato) degli Stati membri? Per (tentare di) rispondere a questo interrogativo, è parso utile analizzare la posizione assunta da tre ordinamenti

38. In carica dal 1° dicembre 2024, la Commissione von der Leyen II ha inserito tra le proprie priorità la questione digitale, con l'obiettivo di implementare efficacemente la normativa da ultimo adottata (il *Digital Services Act* e il *Digital Markets Act*), aumentando al contempo gli investimenti nelle tecnologie chiave, a partire dall'intelligenza artificiale. Per il discorso di insediamento della Presidente Ursula von der Leyen si veda: *Speech by the President at the European Parliament Plenary on the new College of Commissioners and its programme*.

39. Numerosissime sono le definizioni proposte intorno al concetto di *digital sovereignty*. Seppur ormai risalente, ha senso ricordare il contributo offerto da Stephane Couture e Sophie Toupin che ne hanno analizzato i diversi significati proposti, mappando circa cinquanta articoli e testi accademici. Cfr. Couture–Toupin 2019, pp. 2305-2322. Un'operazione analoga, partendo dalla nozione di *data sovereignty*, è stata effettuata da Hummel–Braun–Tretter–Dabrock 2021, pp. 1-17. Ciò detto, pare opportuna una precisazione terminologica relativamente ai concetti di sovranità tecnologica e sovranità digitale, talvolta erroneamente utilizzati come sinonimi. Infatti, secondo Hellmeier e von Scherenberg, mentre la sovranità digitale "si concentra su azioni, competenze e meccanismi di controllo nel mondo digitale", il concetto di sovranità tecnologica è "più ampio" e include "normative e relazioni a livello internazionale". Cfr. Hellmeier–von Scherenberg 2023, pp. 9-10. L'accezione attribuita, in particolare al concetto di *technology sovereignty*, dalle istituzioni europee è ben chiarita da Edler 2024.

40. A tal proposito, si veda anche European Commission 2020.

41. Cfr. Celeste 2021-a, p. 180.

europei in particolare: la Francia, la Germania e l'Italia. La ragione della scelta dei primi due Paesi è presto detta: la Francia e la Germania sono, tra gli Stati membri dell'Unione, quelli che maggiormente si sono impegnati nel campo della sovranità digitale, promuovendo sin dal principio un discorso strategico a livello nazionale. Inoltre, lo Stato francese e quello tedesco hanno stipulato tra loro diverse intese finalizzate a realizzare programmi congiunti in materia digitale[42]. La *ratio* di inserire l'Italia nell'alveo della comparazione va, invece, ricercata nelle peculiari caratteristiche assunte dal dibattito sulla sovranità digitale nel nostro Paese, arrivando quasi ad assumere una biforcazione di significati nell'indirizzo politico promosso dal Governo e nei discorsi politici pronunciati dal Presidente della Repubblica.

3.1. Francia: *souveraineté, marché, sécurité*

Non è certo un mistero che in Francia l'interesse intorno al tema della sovranità digitale, la *souveraineté numérique*, abbia incrociato la prospettiva europea. È stato proprio il Presidente della Repubblica francese Emmanuel Macron ad invocare, durante l'*Internet Governance Forum* di Parigi del 2018, la creazione del citato modello europeo di governance di Internet, basato su forme di regolamentazione democratica[43]; così come, nel giugno 2020, è stata la Francia (insieme alla Germania) a perorare il progetto Gaia-X per la creazione di una piattaforma di *cloud computing* europea basata sui valori dell'Ue[44].

Ben prima di quegli anni, va detto, la nozione di sovranità digitale – oltre ad essere utilizzata in numerosi discorsi politici e della stampa[45] – era stata posta a fondamento del progetto *Andromède*, relativo allo sviluppo di un ecosistema digitale incentrato su un "cloud sovrano" e lanciato dal governo francese nel 2011 con l'obiettivo di competere economicamente con le imprese estere in un mercato percepito come promettente. "Il faut absolument que nous soyons capables de développer une alternative française et européenne dans ce domaine, qui connaît un développement exponentiel, que les Nord-Américains dominent actuellement", aveva sostenuto con forza il Primo Ministro François Fillon al momento della presentazione del progetto[46]. D'altra parte, l'obiettivo di promuovere l'industria francese nel settore tecnologico per contrastare il monopolio americano era stato dichiarato in tempi non sospetti, quando nel 1966, sotto la Presidenza di De Gaulle, venne istituita una Commissione col compito di varare un *Plan Calcul*, un piano informatico per lo Stato francese[47].

Arenatosi a causa del mancato raggiungimento di un accordo tra due dei tre partner coinvolti nell'iniziativa, *Andromède* è stato rimpiazzato nell'anno successivo da due diverse proposte (*Cloudwatt* e *Numergy)*, che, pur formalizzatesi in un'infrastruttura tecnologica operante grazie soprattutto all'ingente finanziamento predisposto dallo Stato

42. Da ultimo, ad esempio, i due Paesi hanno sottoscritto una dichiarazione d'intenti comune finalizzata a rinforzare la cooperazione nell'ambito della sovranità digitale e amministrazione pubblica.
43. Cfr. Macron 2018.
44. Come noto, la realizzazione del progetto Gaia-X è andata incontro a numerosi ostacoli: il coinvolgimento nell'iniziativa dei *big player* americani (AWS, Microsoft, Google, IBM) e cinesi (Huawei), ha indotto diversi partner europei ad abbandonare, ritenendo che le interferenze straniere facessero venire meno la ragion d'essere di Gaia-X. D'altronde, come hanno evidenziato Francesco Amoretti e Mauro Santaniello, è decisamente "difficile e complesso realizzare le condizioni di esercizio di un potere sovrano in un mondo, come quello digitale, caratterizzato da interdipendenze, *path dependencies* ed effetti di scala e di network". Cfr. Amoretti–Santaniello 2024, p. 39.
45. È interessante, a tal proposito, notare la mutazione che ha riguardato il concetto di sovranità digitale nel dibattito pubblico francese: dall'espressione *souveranité* – che trasmette l'idea secondo cui qualsiasi servizio o tecnologia digitale deve essere svolto esclusivamente a livello nazionale – si è passati a *confiance*, termine che sta ad indicare l'adozione di una prospettiva euro-rivolta, per cui le ambizioni digitali francesi si realizzano nel più ampio quadro dell'Unione europea. Sul punto Desforges 2023, pp. 127-133.
46. Cfr. Fillon 2010.
47. Cfr. Institut d'Histoire de l'Industrie 1998.

francese, si sono arrestate dopo un iniziale periodo di funzionamento [48].

Le motivazioni che hanno accompagnato la (tentata) nascita del *cloud à la française*, inducono a pensare che lo sviluppo di un ecosistema digitale in Francia si sia saldato, almeno agli inizi, ad una dimensione per lo più economica. Tale carattere, d'altra parte, viene in luce altresì dai contenuti del *New Industrial France* del 2013[49] sostenuto dall'allora Ministro dell'economia e della ripresa industriale Arnaud Montebourg. I trentaquattro piani di ripresa nazionali di cui si componeva il programma trattavano la materia digitale sotto diversi aspetti (*Big data*, *Cloud computing, Cybersecurity*, ecc.), ma ognuno di loro era per lo più connesso all'esigenza di tutela nei confronti dello spionaggio economico estero e, in maniera solo incidentale, all'opportunità di prevedere un sistema di protezione dei dati personali e dei dati strategici aziendali.

A segnare un'inversione di rotta, spostando i riflettori sul tema della sicurezza, sono state le clamorose rivelazioni effettuate da Edward Snowden nel giugno 2013 sulla massiccia attività di sorveglianza messa in atto da parte della *National Security Agency* (NSA) nei confronti dei cittadini statunitense e non solo. Il c.d. *datagate*, in Francia come altrove nel mondo, ha suscitato un'ondata di indignazione tale da tradursi nell'adozione (o quanto meno nella proposizione) di numerose iniziative in materia di sicurezza digitale. Pochi mesi dopo lo scandalo, nel febbraio 2014, l'allora Ministro della difesa francese Jean-Yves Le Drian si è fatto infatti promotore del *Pacte défense cyber,* "50 mesures pour changer d'échelle", una strategia di cybersecurity che postulava un approccio "a cerchi concentrici"[50] con un primo livello di pertinenza dei sistemi interni del Ministero, un secondo relegato al settore industriale per lo sviluppo di soluzioni nazionali e un terzo contemplante una collaborazione con l'Unione europea.

Dunque, una strategia che, pur privilegiando l'approccio nazionale, non escludeva di ricorrere a soluzioni europee quando necessario, evitando la dipendenza da attori extra-Ue. La volontà della Francia di mantenere il controllo sulle tecnologie digitali senza isolarsi dalla prospettiva di una cooperazione europea è stata, peraltro, confermata dal ruolo chiave che il Paese ha assunto nell'adozione degli ultimi atti europei in materia, i già citati *Cybersecurity Act*, *Digital Services Act* e *Digital Markets Act*. Il disegno digitale francese, dunque, non sembrerebbe tanto volto a "promuovere l'indipendenza totale o l'autarchia, ma [ad] esprimere il desiderio di scegliere liberamente alleanze per garantire l'autonomia strategica della Francia"[51], che comunque si inserisce nel quadro della ricerca di un'autonomia strategica europea.

Ciò detto, per quanto l'asse Francia-Ue sia evidentemente solido nelle strategie di governance di Internet, nell'approccio francese alla *souveraineté numérique* viene in rilievo una marcata attenzione alla dimensione economica, correlata alle opportunità intraviste nel mercato della *cybereconomy*, e a quella securitaria, che si esplica soprattutto nell'ambito della difesa avverso le ingerenze straniere nel dominio della rete; decisamente meno forte pare essere, invece, l'*appeal* esercitato dal tema della tutela virtuale dei diritti fondamentali *lato sensu*. In quest'ottica, la *Loi pour une République numérique* (*Loi n° 2016-1321 du 7 octobre 2016*), approvata nell'alveo dell'applicazione del GDPR, rappresenta un'occasione mancata. Ad una denominazione altisonante, iperbolica, come definita dal Consiglio di Stato, non è corrisposta la predisposizione di contenuti di egual spessore, essendo assente sia la previsione di nuovi strumenti giuridici di tutela (la legge si limita ad approfondire meccanismi già esistenti) sia una seria riflessione sul tema della sovranità digitale[52]. Grossomodo, una simile considerazione può essere mossa altresì nei confronti della *Loi numérique* (*Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et*

48. Sul punto Henni 2015.
49. Cfr. Montebourg 2013.
50. Cfr. Desforges 2023, p. 166.
51. Così Danet–Desforges 2020, p. 195.
52. Un'analisi approfondita dei contenuti della Loi n° 2016-1321 du 7 octobre 2016 è stata proposta da Cluzel–Métayer 2017.

à réguler l'espace numérique), entrata in vigore nel maggio 2024, la quale, oltre a limitarsi a ripetere il testo dei neonati regolamenti europei DMA e DSA, appare "estremamente tecnica, poco intellegibile e non sempre rispondente ad un filo logico"[53].

Tutto ciò fa certamente perdere di senso alle importanti dichiarazioni rilasciate da Emmanuel Macron in occasione del *Forum de Paris sur la paix* del 2018, nell'ambito del quale, tra le altre cose, aveva espressamente collegato la regolazione dello spazio digitale alla finalità di creare "tecnologie per il bene comune"[54]. Tema questo che, a mio dire, merita un ben più ampio spazio di riflessione rispetto a quello che gli si potrebbe offrire in questo scritto e che, pertanto, ci si riserva di approfondire in altro momento.

3.2. Germania: *für eine kollektive und individuelle (wirtschaftliche) digitale Souveränität*

Che la Germania abbia occupato, parimenti alla Francia, un ruolo di prim'ordine nell'affermazione del concetto di sovranità digitale a livello europeo è stato detto. Per corroborare quest'affermazione basti qui giusto ricordare la centralità riconosciuta all'obiettivo di "expand the EU's digital sovereignty"[55] dalla presidenza tedesca del Consiglio dell'Unione nel luglio 2020. Tuttavia, a differenza della Francia, dove come si è visto le prime iniziative sull'autonomia tecnologica sono piuttosto datate, in Germania i discorsi sulla *digitalen Souveränität* hanno iniziato a prender forma solo a partire dal 2013 come conseguenza delle rivelazioni di Edward Snowden.

Risale a quell'anno, infatti, la presentazione da parte di *Deutsche Telekom* di un progetto per la creazione di un *Internetz*, un Internet pensato per instradare solo in tedesco tutti i dati sul traffico a livello nazionale[56]; proposta che ha seguito la sospensione del rilascio di autorizzazioni per il trasferimento di dati dalla Germania a paesi non Ue da parte della Conferenza delle Autorità Nazionali Tedesche per la Protezione dei Dati[57].

Il c.d. "effetto Snowden" in terra tedesca non si è però limitato a questo: nel dicembre 2013 è stato, infatti, stipulato un contratto di coalizione tra i partner di governo CDU/CSU e SPD, incentrato primariamente sull'attuazione di "misure per riconquistare la sovranità tecnologica" al fine di proteggere la libertà e la sicurezza in rete[58]. Tali misure includevano anche l'elaborazione della *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* (anche conosciuta come *IT-Sicherheitsgesetz*, Legge sulla sicurezza IT)[59], entrata in vigore nel 2015 e successivamente emendata nel 2021, contenente obblighi per i gestori di infrastrutture critiche (come l'energia, l'acqua, la sanità o le telecomunicazioni) in relazione all'aumento della sicurezza informatica delle rispettive reti. A due anni di distanza, poi, e più esattamente nell'aprile 2017, una nuova iniziativa governativa ha dato vita al *Zentralen Stelle für Informationstechnik im Sicherheitsbereich* (*ZITiS*), l'Ufficio Centrale per la Tecnica dell'Informazione nel Settore della Sicurezza, con il compito principale di supportare le agenzie di sicurezza nel trattamento delle tecnologie informatiche e nella gestione delle informazioni digitali, con particolare attenzione alla sicurezza nazionale. Sempre per mano del Governo, inoltre, nel 2021 è stata fondata l'*Agentur für Innovation in der Cybersicherheit* (*Cyberagentur*), l'Agenzia per

53. Per una critica della *Loi numérique* si veda Mouron 2024, pp. 35-39.
54. Cfr. *Appel de Paris pour la confiance et la sécurité dans le cyberespace*, Paris Peace Forum.
55. Cfr. Presidenza tedesca del Consiglio dell'Unione europea 2020.
56. Cfr. Hon–Millard–Singh et al. 2016.
57. Cfr. *Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24 Juli 2013*.
58. Cfr. CDU–CSU–SPD 2013. In particolare, la politica digitale del governo costituitosi sulla base di tale accordo venne organizzata nei Dipartimenti dell'Economia, dell'Interno e dei Trasporti, foriero ciascuno di misure contemplanti diversi obiettivi: il Ministero dell'Interno fece suo il tema della sicurezza dell'infrastruttura digitale; quello dei Trasporti si pose come priorità la promozione della guida automatizzata e connessa e l'espansione dell'infrastruttura a banda larga; il Ministero federale dell'Economia perseguendo un concetto di politica digitale più ampio rispetto gli altri due, nel marzo 2016 adottò la "Strategia digitale 2025" elencando complessivamente dieci campi d'azione. Per un approfondimento sul punto si rimanda a Misterek 2017.
59. Per un commento alla legge si rimanda a Hilgert 2015.

l'innovazione nella sicurezza informatica, con lo scopo di sviluppare tecnologie di sicurezza informatica con vantaggi strategici per la sicurezza interna ed esterna e, quindi, con l'obiettivo di rafforzare le tecnologie e i sistemi informatici tanto a livello nazionale quanto in prospettiva europea, "garantendo così la sovranità tecnologica della Germania e dell'Europa"[60]. Negli ultimi anni, invece, il discorso sulla *digitalen Souveränität* sembra aver incrociato maggiormente la prospettiva della digitalizzazione delle pubbliche amministrazioni, in modo da ridurre le "dipendenze dai fornitori di software nell'amministrazione federale" e di garantire "l'indipendenza del produttore" nell'amministrazione pubblica.

L'insieme di queste disposizioni evidenzia la palese volontà, da parte degli organi di governo tedeschi, di attribuire una dimensione marcatamente economica al concetto di sovranità digitale, dal momento che le stesse (disposizioni) sono nate con lo scopo di proteggere l'infrastruttura informatica e i dati delle aziende tedesche, da un lato, e di promuovere la competitività e l'indipendenza tecnica della Germania come sede commerciale e tecnologica, dall'altro.

Il paradigma economico, peraltro, viene in rilievo anche in una seconda dimensione – del tutto peculiare – che connota la strategia digitale tedesca: quella individuale. Un gran numero di raccomandazioni volte a rafforzare la sovranità digitale tedesca tratta il tema dell'alfabetizzazione digitale e, più in generale, richiama l'attenzione sui diritti dei cittadini (*rectius* dei consumatori) in rete. In effetti, la necessità di proteggere la *sovranità* degli individui nel loro ruolo di consumatori di servizi digitali è stata sottolineata in Germania ben prima dell'inizio del dibattito politico sulla sovranità digitale. La *Charta Verbrauchersouveränität in der digitalen Welt*, "Carta della sovranità dei consumatori nel mondo digitale", redatta dal Ministero federale per l'alimentazione, l'agricoltura e la protezione dei consumatori nel 2007, sottolineava l'importanza della sicurezza informatica come garanzia del diritto alla "autodeterminazione informativa". Oggi, invece, la tutela della sovranità dei consumatori digitali si esplica principalmente nelle opportunità offerte ai cittadini di utilizzare le tecnologie e i contenuti digitali in modo responsabile e autodeterminato, tant'è che nel 2017 il *Sachverständigenrat für Verbraucherfragen* (Consiglio consultivo tedesco per gli affari dei consumatori) ha definito la sovranità digitale come "capacità di agire e libertà di decisione dei consumatori nel mondo digitale, assumendo diversi ruoli: come attori di mercato, come cittadini consumatori all'interno della società e come *prosumer* nei social network"[61].

Oltre alla sovrapposizione della dimensione individuale ed economica della sovranità digitale, è stata osservata anche una fusione con la dimensione statale[62].

In ultima analisi, la dimensione statale e quella individuale sembrano coesistere nella strategia tedesca della *digitalen Souveränität*, entrambe tuttavia si sviluppano sotto l'egida del paradigma economico. Pertanto, l'attenzione ai diritti individuali online non può dirsi rientrare nell'alveo della tutela dei diritti fondamentali generalmente intesi, in quanto l'individuo – essendo concepito come consumatore – acquisisce dignità di tutela perché strumentale alla salvaguardia del mercato.

3.3. Italia: la "Agenda Digitale Mattarella"

Il contributo dell'Italia al discorso sulla sovranità digitale è ben più esiguo rispetto a quello fornito delle vicine Francia e Germania. Una timidezza, quella italiana, che non si riscontra solo nell'apporto offerto al dibattito europeo, ma trova un suo riflesso anche nelle politiche nazionali. L'attuale esecutivo, in carica dall'ottobre 2022, ha inaugurato il suo "corso digitale" con la

60. Cfr. Boeck 2018.

61. Cfr. Pohle 2020, p. 16. Della stessa Autrice si veda anche Pohle–Thorsten 2021, pp. 319-340.

62. Julia Pohle riporta l'esempio di come, nella discussione sugli aspetti della sicurezza e della politica interna, l'uso autodeterminato dei servizi e delle tecnologie digitali venga presentato come un prerequisito per cittadini e lavoratori responsabili e digitalmente sovrani. A tal proposito ricorda che nel documento tematico sulla sovranità digitale della pubblica amministrazione, l'*IT Planning Council* – l'organo direttivo politico dei governi federale e statale per il coordinamento IT – definisce la sovranità digitale come "le capacità e le possibilità degli individui e delle istituzioni di essere in grado di esercitare il loro ruolo nel mondo digitale in modo indipendente, autodeterminato e sicuro". Cfr. Pohle 2020, p. 17.

soppressione del Ministero dell'innovazione tecnologica e la transizione digitale (MITD)[63], concentrando principalmente i propri sforzi in materia sull'ammodernamento digitale delle pubbliche amministrazioni e sulla realizzazione di infrastrutture di rete a banda larga, entrambi rientranti negli obiettivi del PNRR. Si può dire infatti che il *Piano Nazionale di Ripresa e Resilienza* (PNRR) – il pacchetto di investimenti e riforme predisposto dal Governo italiano nell'ambito del *Next Generation EU*, il programma voluto dall'Unione europea per favorire il rilancio degli Stati membri dopo la pandemia Covid-19 – sia stato, insieme ai regolamenti Ue, l'insieme di misure che maggiormente ha inciso sull'ambito digitale in Italia.

Non una grande attenzione è stata quindi rivolta alla *digital challeng*e nel nostro Paese. Di più, alcuni recenti fatti di cronaca hanno indotto a pensare che il progetto di sovranità digitale europea possa essere minato proprio dal più "sovranista", per sua stessa ammissione, dei governi dell'Ue[64].

In questo contesto di apparente abulia (se non addirittura tentata contrarietà), una posizione del tutto differente è occupata dal Presidente della Repubblica Sergio Mattarella. Facendo sua una narrazione fondata su assiomi euro-rivolti, Mattarella ha dedicato grande attenzione alla questione, sviluppando – si può dire – una sorta di personale "Agenda Digitale". In numerosi discorsi, anche piuttosto risalenti, egli ha infatti posto l'accento sui temi legami al mondo virtuale, e precipuamente sul concetto di sovranità digitale, attribuendovi un'accezione analoga a quella maturata nel contesto dell'Unione europea, dove – come si è visto – costituzionalismo e sovranità digitale trovano una loro sintesi.

In occasione del XV simposio COTEC Europa[65] "Culture meets innovation", tenutosi a Braga nel maggio 2022, il Presidente della Repubblica, nell'incentrare il suo discorso sul legame indissolubile tra innovazione e cultura, ha evidenziato la necessità di imprimere un'accelerazione al "raggiungimento di una *sovranità europea* […] per quanto riguarda il campo tecnologico", interrogandosi, al contempo, su come fare a ribadire la centralità della persona in modelli determinati "da superintelligenze dallo sviluppo potenzialmente autonomo", con un esplicito riferimento all'intelligenza artificiale e al *machine learning*[66].

Due anni dopo – nella XVII edizione del simposio COTEC tenutosi a Las Palmas de Gran Canaria nel settembre 2024 dall'emblematico titolo "Sovranità tecnologica" – Mattarella ha, quindi, ripreso e approfondito le sue riflessioni. Perorando

63. Le funzioni del MITD, riabilitato all'avvio del Governo c.d. "Conte-II" e rafforzato dall'Esecutivo c.d. "Draghi", sono state delegate dalla Presidente del Consiglio Giorgia Meloni al Sottosegretario alla Presidenza del Consiglio con delega alla Transizione digitale Alessio Butti.

64. Sono a tutti note le indiscrezioni fatte trapelare dall'agenzia di stampa *Bloomberg* sull'accordo che sarebbe stato concluso tra la Presidente del Consiglio Meloni e Elon Musk per un (decisamente cospicuo) investimento italiano nella sua società di telecomunicazioni *SpaceX*. Va comunque precisato che la notizia è stata smentita con fermezza in una nota di Palazzo Chigi del 6 gennaio 2025: "La Presidenza del Consiglio dei ministri smentisce che siano stati firmati contratti o presi accordi tra il Governo italiano e la società *SpaceX* per l'utilizzo del sistema di comunicazione satellitare *Starlink*". Cfr. Governo Italiano – Presidenza del Consiglio dei Ministri, *Sistema di comunicazioni satellitari Starlink, la nota di Palazzo Chigi*, 6 gennaio 2025. A tal proposito si ricordi che l'Unione europea ha avviato, oramai da diversi anni, una propria politica spaziale: Consiglio europeo, *Politica spaziale dell'UE*.

65. La "Fondazione COTEC" è stata costituita in Italia – sul modello *Fundación Cotec* di Spagna e parallelamente all'*Associação Cotec* del Portogallo – il 21 aprile 2001 al fine di "incoraggiare e promuovere azioni finalizzate al miglioramento della competitività tecnologica dell'Italia e di individuare le migliori politiche pubbliche per ottimizzare il patrimonio della ricerca e rafforzare le capacità industriali del nostro Paese". La collaborazione tra le tre Fondazioni si sostanzia nei Simposi annuali, durante i quali i Capi di Stato dei tre Paesi – che le presiedono – si incontrano "per delineare azioni comuni sui temi della politica dell'Innovazione ed attivare iniziative specifiche di collaborazione". Per maggiori informazioni sulla storia e gli obiettivi della Fondazione COTEC consultare il relativo sito web.

66. Cfr. *Intervento del Presidente della Repubblica Sergio Mattarella al XV Simposio COTEC Europa "Culture meets innovation"*.

l'importanza della realizzazione nell'ambito delle nuove tecnologie di "campioni europei espressione di sovranità condivisa", ha incitato a colmare il divario rispetto alle grandi potenze tecnologiche rappresentate dagli Stati Uniti e dalla Cina. A questo proposito, ha però specificato che sovranità tecnologica non significa chiusura, arroccamento o protezionismo – atteggiamenti che comporterebbe un ulteriore indebolimento e marginalizzazione dell'Unione europea e dei suoi Stati membri – al contrario, è un cantiere in cui potenziare la ricerca per affrontare con coraggio le sfide della transizione tecnologica. Sempre in quest'occasione, ha poi posto l'accento sui rischi derivanti dalle nuove tecnologie per l'esercizio della libertà da parte dei singoli individui[67].

Ma non si è limitato alle suddette affermazioni. In uno degli ultimi discorsi, pronunciato in occasione del dottorato *honoris causa* conferitogli dall'Università di Aix-Marseille il 5 febbraio 2025, Mattarella ha sostenuto con fermezza la necessità di guardarsi dai "neo-feudatari del Terzo millennio – novelli corsari a cui attribuire patenti – che aspirano a vedersi affidare signorie nella dimensione pubblica, per gestire parti dei beni comuni rappresentati dal cyberspazio nonché dallo spazio extra-atmosferico, quasi usurpatori delle sovranità democratiche"[68].

Riferimenti a fatti e persone (non) sono puramente casuali.

Il fulcro delle dichiarazioni del Presidente Mattarella si sostanzia, può concludersi senza timore di essere smentiti, nell'intreccio tra aspirazioni alla sovranità tecnologica, intesa come propulsore di sviluppo e garanzia di sicurezza, e necessità di tutela dei diritti fondamentali in rete. In questo senso, la sua posizione è certamente, tra le prospettive qui indagate, quella che maggiormente si avvicina alla direzione intrapresa dall'Unione europea. Bisogna però attribuirle la valenza che le spetta: vale a dire la linea di pensiero del Presidente della Repubblica, una figura che – all'interno di una forma di governo parlamentare qual è quella italiana – può avere al più una funzione "esortativa" rispetto alle scelte in merito all'indirizzo politico, la cui definizione resta nelle mani dell'Esecutivo[69].

Quello che avviene in Italia è (quanto meno) singolare.

4. Sovranità digitale *versus* costituzionalismo digitale

L'analisi finora condotta, che non ha pretesa di esaustività alcuna[70], rende possibile una prima riflessione sulla diramazione che ha assunto il discorso su sovranità e costituzionalismo digitale negli (in alcuni, meglio) Stati membri dell'Ue, consentendo di comprendere come i singoli interessi nazionali si collochino rispetto al progetto europeo.

L'Unione europea ha costruito una narrazione contemplante una sfera digitale basata sui valori comuni europei, con al centro gli individui e i loro diritti, che si realizza mediante l'implementazione di interventi normativi volti a plasmare una "tecnologia per la gente" (*Tech that works for people*)[71]; lo si è detto chiaramente. Rispetto questa narrazione la prima contro-tendenza che viene

67. Cfr. *Intervento del Presidente della Repubblica Sergio Mattarella al XVII Simposio COTEC Europa "Sovranità tecnologica"*, 20 settembre 2024.
68. Cfr. *Intervento del Presidente della Repubblica Sergio Mattarella alla Cerimonia di consegna dell'onorificenza accademica di Dottore honoris causa dall'Università di Aix-Marseille: «L'ordre international entre règles, coopération, compétition et nouveaux expansionnismes»*, 5 febbraio 2025.
69. Questo è quel che sancisce l'art. 95 della Costituzione. Tuttavia, non ci si può esimere dal ricordare che le vicende caratterizzanti il corso della storia repubblicana italiana degli ultimi decenni hanno mostrato un potenziale cambiamento di ruolo del Presidente della Repubblica. La dottrina sulla figura presidenziale è consistente; si rimanda qui, per un commento agli eventi che hanno caratterizzato il I settennato di Mattarella e la conseguente evoluzione della sua figura nella forma di governo parlamentare, a Spiniello 2022, pp. 135-148.
70. Quanto esposto in questo contributo non è altro che il frutto di una prima riflessione su un tema in continuo divenire. Pertanto, ci si riserva di approfondirlo in un successivo scritto, con l'intento altresì di ampliare lo spettro della comparazione, estendendo l'analisi del concetto di sovranità digitale ad altri Stati membri dell'Ue.
71. Si veda, in tal senso, la già citata *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, il cui primo capitolo si intitola significativamente "Mettere le persone al centro della trasformazione digitale".

in luce nelle strategie nazionali dei Paesi in esame (principalmente Francia e Germania) è l'assenza, pressoché totale, di riferimenti al tema della tutela dei diritti fondamentali; se non per quel che concerne la dimensione securitaria (il dato-individuo in Francia) o di mercato (l'individuo-consumatore in Germania). Diverso è il caso dell'Italia, dove, al contrario, ampio spazio è riconosciuto alla protezione della *persona virtuale* (e, dunque, ai suoi diritti e libertà in rete); tuttavia, ciò avviene in un ambito puramente speculativo, quale può essere quello dei discorsi presidenziali, non trovando una corrispettiva traduzione pratica nella messa a punto di una strategia governativa.

Il secondo dato da estrapolare vive nella forte matrice economica che denota, in generale, le iniziative in materia digitale. È vero che i dati e le infrastrutture digitali sono visti come *asset* di importanza critica per lo sviluppo economico europeo e che, quindi, l'*European digital sovereignty* ha anche (e certamente) una sua connotazione economica; tuttavia, a livello nazionale lo spazio virtuale sembra essere considerato esclusivamente come uno spazio economico, un luogo in cui promuovere essenzialmente la competitività e l'indipendenza tecnica delle aziende e delle infrastrutture statali. Ciò avviene in Francia, sin dai tempi di *Andromède*, in Germania, con l'insieme di risposte normative alle rivelazioni di Snowden e, in maniera minore, in Italia, per quel concerne l'efficientamento delle pubbliche amministrazioni.

Tali accezioni – finendo col restringere il perseguimento della sovranità digitale a una pura strategia economica e di sicurezza – fanno fatica a combinarsi con la prospettiva europea e rischiano, addirittura, di capovolgerla, arrivando all'antitetico approdo per cui la sovranità digitale si struttura *versus* il costituzionalismo digitale. Il cieco inseguimento di un paradigma economico-securitario rischia infatti di risolvere il bilanciamento tra il perseguimento degli interessi economici, la ricerca di sicurezza "a tutti i costi" e la richiesta di tutela dei diritti individuali – operazione già di per sé estremamente delicata e ancora più complessa nell'ecosistema digitale, con un contesto ancora tutto da definire – in una mera sovrapposizione dei primi sui secondi. Questioni come la libertà di manifestazione del pensiero online o la libertà di riunione e associazione virtuale – tanto care al costituzionalismo digitale – diventerebbero di second'ordine, eclissate da logiche di mercato e protezioniste.

A questa riflessione, è poi da aggiungere una considerazione di carattere più generale sugli effetti che l'esercizio di un'eccessiva forza centripeta è potenzialmente in grado di produrre: sovvenzionare la creazione di infrastrutture digitali all'interno dei singoli territori nazionali, svincolate da un quadro sovranazionale comune, equivale ad alimentare tendenze isolazioniste col rischio di tramutare le rivendicazioni in ordine alla sovranità digitale in forme di bieco sovranismo. D'altra parte, tali pericoli sono stati evidenziati anche in relazione alla strategia dell'Unione europea in materia di trattamento dei dati personali: le politiche di localizzazione dei dati, generando costi elevati connessi al trasferimento dei centri dati in Europa, sono suscettibili di alterare il corso dell'economia globale[72]. Così declinata, la sovranità digitale corre il rischio di esacerbare le tensioni politiche ed economiche con gli Stati terzi, "portando ad uno strenuo braccio di ferro che, in ultima analisi, non migliora la protezione dei dati europei" e non favorisce l'economia interna[73].

Peraltro, non è da escludere (ma, al contrario, è assai probabile) che le rivendicazioni digitali nazionali possano approdare in tensioni tra le regole Ue e il diritto costituzionale interno, che, pur dovendosi risolvere in ossequio al principio del primato del diritto dell'Unione, minerebbero inesorabilmente il progetto di trasformazione digitale europeo, essendo esso strettamente connesso all'unità di intenti degli Stati membri.

5. Costituzionalismo digitale: suona già come un anacronismo?

Le diverse dimensioni della sovranità e del costituzionalismo digitale paiono essere destinate ad una irrimediabile competizione reciproca. La concezione dominante di *digital sovereignty* affermatasi negli Stati nazionali si costruisce in relazione agli obiettivi di politica economica e di sicurezza, secondo una logica che confonde la protezione

72. In argomento Mishra 2015.

73. Cfr. Celeste 2021-a, p. 15.

col protezionismo e che mortifica le aspirazioni in ordine al rispetto dei diritti digitali.

In un simile contesto, sembra lecito domandarsi: è ancora tempo di costituzionalismo digitale?

Ernst Forsthoff, in un volume datato 1971[74], imputava alla perdita della funzione regolatrice delle Costituzioni – di fronte a uno Stato ridotto a un'entità amministrativa, priva di qualsiasi forza politica e subordinata alle esigenze della tecnica – la causa dello *smarrimento* degli individui, in balia (delle) e indifesi (di fronte alle) rivendicazioni dei grandi attori privati. "L'elemento di potere dei prodotti della tecnica" – scriveva più precisamente Forsthoff – "si manifesta così nella naturale opposizione di questa all'ideologia delle libertà"[75].

Shoshana Zuboff, ad oltre cinquant'anni di distanza, in uno scritto destinato anch'esso a restare nella storia[76], riferendosi all'azione messa a punto dalle *Big Tech* americane nell'affermazione di ciò che definisce il *capitalismo della sorveglianza*, ha sostenuto che la Costituzione statunitense è stata "sfruttata come scudo per una serie di pratiche innovative che sono antidemocratiche per fini e conseguenze, e di fatto distruggono i valori del primo emendamento, finalizzati a proteggere l'individuo da ogni abuso di poteri"[77].

Uno denuncia l'assenza della capacità operativa della Costituzione, l'altra l'uso strumentale che ne è stato fatto. Entrambi, ad ogni modo, colgono lo strettissimo nesso tra i contenuti (e la tenuta) delle Carte fondamentali e la regolazione delle tecnologie, nuove o vecchie che siano.

Il rapporto tra diritto e tecnologie – lo si è ricordato – non è certo esclusivo affar di oggi, ma è oggi che esso ha assunto una configurazione *trittica*, con l'inclusione di un terzo soggetto nella relazione: i poteri privati, o, più esattamente, il monopolio esercitato dai poteri privati in rete. Ed è proprio l'emersione dei *CyberSovrani* che, se per un verso pone il costituzionalismo dinnanzi a sfide inedite e complesse, per altro verso ne rivela tutta la necessaria ragion d'essere. Il "fondamento utopico"[78] che ha accompagnato la sua nascita – *limitare il sovrano* e, quindi, ridistribuire i poteri e garantire i diritti – non fa che trovarsi rafforzato negli scopi che la conformazione dell'ecosistema digitale gli impone di perseguire. Compito del costituzionalismo digitale è, cioè, trovare il modo di "regolare un potere che è distribuito tra molti attori all'interno di sistemi complessi con molte componenti separate che interagiscono. Allo stesso tempo, deve anche assicurare che ci siano appropriati limiti esterni all'autonomia di questi sistemi che riflettano le aspettative di legalità tipiche del pensiero democratico"[79].

È evidente che, in tempi di digitalizzazione, l'attenzione all'economia e alla sicurezza non può rendere giustizia alle complesse questioni che si riconnettono all'esercizio dei diritti e delle libertà dell'individuo. Il diritto alla libertà di espressione, la tutela dei minori, della reputazione e, *ça va sans dire*, della privacy, sono solo alcuni dei principi che entrano in gioco nella regolamentazione del virtuale. Per questo la strategia europea, il tentativo di normare lo spazio digitale intersecando i principi della sovranità e del costituzionalismo digitale – che comunque non è esente da contraddizioni[80] – resta la più interessante proposta in campo. Da questo punto di vista, attualmente la vera sfida non consiste tanto nel continuare ad incrementare la produzione normativa sul digitale – che, allora sì, rischierebbe di diventare ipertrofica ed eccessivamente frammentata – quanto piuttosto nel darvi applicazione, per evitare che resti lettera morta. Tale applicazione, peraltro, dovrebbe essere retta

74. Forsthoff 1971/2011.

75. *Ivi*, p. 33.

76. Zuboff 2019.

77. *Ivi*, p. 79.

78. Cfr. Azzariti 2013, p. 188.

79. Cfr. Cavani 2023, p. 247.

80. (Almeno) tre sono gli ordini di problemi a cui va incontro il progetto europeo a detta di Amoretti e Santaniello: la difficile operabilità del modello, come già evidenziato in precedenza, a causa della natura interrelazionale dell'ecosistema digitale; lo scontro tra la tutela dei diritti fondamentali in rete e il processo di crescente securitizzazione del cyberspazio; l'ampliamento del divario tra Nord e Sud del mondo (Europa vs. Africa) conseguente all'implementazione di politiche digitali eurocentriche. Cfr. Amoretti–Santaniello 2024, pp. 39-40.

da *standard* uniformi sia per quel che riguarda l'implementazione delle normative a livello nazionale – in questo senso, si condivide la critica di chi ha denunciato l'eccessivo numero di clausole aperte contenute negli ultimi regolamenti Ue, cosa che paia lasciare un margine di manovra eccessivo agli Stati membri[81] – sia per quanto concerne il principio della certezza del diritto. Ciò a cui si è assistito nella prima fase dell'affermazione dei diritti digitali, un legislatore inerme e dei giudici (soprattutto europei ma anche nazionali) iperattivi, non può diventare la regola: è necessario che le figure e i livelli oggetto di sanzione giurisdizionale muovano in un quadro di legislazione certa e uniforme.

Ciò precisato, resta il fatto che è proprio nel perseguimento dell'intreccio tra sovranità e costituzionalismo digitale che vive una preziosa opportunità politica e culturale per affrontare la questione cruciale della distribuzione del potere e delle disuguaglianze (digitali) derivanti dalle nuove gerarchie e dalle attuali dinamiche geopolitiche.

A questo punto, mi pare, la domanda iniziale si risponda da sé: è ancora tempo di costituzionalismo digitale e, per riallacciarmi a quanto scritto in conclusione del primo paragrafo, ne abbiamo bisogno, più che mai.

Riferimenti bibliografici

A. Alpini (2022), *La sovranità digitale europea*, in "TIGOR. Rivista di scienze della comunicazione e di argomentazione giuridica", 2022, n. 2

C. Amalfitano, F. Ferri (2024), *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. Torino, S. Zorzetto (a cura di), La trasformazione digitale in Europa. Diritti e principi, Giappichelli, 2024

F. Amoretti, M. Santaniello (2024), *Sovranità e costituzionalismo digitale*, in B. Henry, S. Vaccaro (a cura di), "Tecnologia, Politica, Società", Mimesis, 2024

G. Azzariti (2022), *Stefano Rodotà e l'uso costituzionalmente orientato delle nuove tecnologie*, in "Costituzionalismo.it", 2022, n. 2

G. Azzariti (2013), *La costituzione come norma e la crisi del costituzionalismo contemporaneo*, in "Rivista Italiana per le Scienze Giuridiche", 2013, n. 4

G. Azzariti (2011), *Internet e costituzione*, in "Politica del diritto", 2011, n. 3

R. Baratta (2019), *Droits fondamentaux et "valeurs" dans le processus d'intégration européenne*, in "Studi sull'integrazione europea", 2019, n. 2

N.W. Barber (2018), *The Principles of Constitutionalism*, Oxford University Press, 2018

J.P. Barlow (1996), *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, 1996

M. Betzu (2021), *Poteri pubblici e poteri privati nel mondo digitale*, in "Rivista del Gruppo di Pisa", 2021, n. 2

C.M. Bianca (1977), *Le autorità private*, Jovene, 1977

M. Boeck (2018), *Technologiesouveränität erlangen – die neue Cyberagentur*, Bundesministerium der Verteidigung, 24 September 2018

E. Cannizzaro (2018), *Il ruolo della Corte di giustizia nella tutela dei valori dell'Unione europea*, in Aa.Vv., "*Liber amicorum* Antonio Tizzano. De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne", Giappichelli, 2018

81. Sul punto Pollicino 2023, p. 583 nonché De Gregorio 2020, p. 1 ss.

V. Cavani (2023), *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in "Diritto pubblico comparato ed europeo", 2023, n. 1

CDU, CSU, SPD (2013), *Deutschlands Zukunft gestalten: Koalitionsvertrag zwischen CDU, CSU und SPD*, 14 Dezember 2013

E. Celeste (2021), *Costituzionalismo digitale e piattaforme: verso una costituzionalizzazione della* lex digitalis, in "Comunicazionepuntodoc", 2021, n. 25

E. Celeste (2021-a), *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini, E. Celeste, J. Quinn (eds.), "Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty", Hart Publishing, 2021

E. Celeste (2020), *Digital Constitutionalism: The Role of Internet Bills of Rights*, University College Dublin, Sutherland School of Law, 2020

E. Celeste (2018), *Digital Constitutionalism. Mapping the constitutional response to digital technology's challenges*, in "HIIG Discussion Paper Series", 2018, n. 2

L. Cluzel-Métayer (2017), *La loi pour une République numérique: l'écosystème de la donnée saisi par le droit*, in "Actualité juridique Droit administratif", 2017, n. 6

P. Costanzo (2014), *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in Aa. Vv., "Annuario 2012 – Costituzionalismo e globalizzazione", Atti del XXVII Convegno annuale AIC, Salerno, 23-24 novembre 2012, Jovene, 2014

S. Couture, S. Toupin (2019), *What does the notion of "sovereignty" mean when referring to the digital?,* in "New Media & Society", vol. 21, 2019, n. 10

D. Danet, A. Desforges (2020), *Souveraineté numérique et autonomie stratégique en Europe: du concept aux réalités géopolitiques*, in "Hérodote", 2020, n. 177-178

G. De Gregorio (2021), *The rise of digital constitutionalism in the European Union*, in "International Journal of Constitutional Law", vol. 19, 2021, n. 1

G. De Gregorio (2020), *Democratising Online Content Moderation: A Constitutional Framework*, in "Computer Law & Security Review", vol. 36, 2020

A. Desforges (2023), *Souveraineté numérique en France: du débat polarisé aux actes dispersés*, in S. Taillat, A. Cattaruzza, D. Danet (eds.), "La Cyberdéfense. Politique de l'espace numérique", Armand Colin, 2023

M. Esposito (2003), *Profili costituzionali dell'autonomia privata*, Cedam, 2003

J. Edler (2024), *Technology sovereignty of the EU: needs, concepts, pitfalls and ways forward*, in Directorate-General for Research and Innovation, "Science, Research and Innovation performance of the EU 2024 report", 2024

European Commission (2020), *A European Strategy for Data*, 2020

G. Finocchiaro (2015), *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in "Il diritto dell'informazione e dell'informatica", 2015, n. 4-5

F. Fillon (2010), *Déclaration de M. François Fillon, Premier ministre, sur le déploiement de la fibre optique dans les zones moyennement denses, l'affectation d'une part du grand emprunt au très haut débit et l'annonce d'un "tarif abordable" pour les ménages modestes*, 18 janvier 2010

E. Forsthoff (1971/2011), Lo Stato della società industriale, a cura di A. Mangia, Giuffrè, 2011

T.E. Frosini (2019), *Liberté Egalité Internet*, Editoriale Scientifica, 2019

L. Gill, D. Redeker, U. Gasser (2015), *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, Berkman Center Research Publication, 2015, n. 15

T. Gillespie (2018), *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018

D. Grimm (2018), *Constitutionalism: Past-Present-Future*, in "Nomos. Le attualità nel diritto", 2018, n. 2

A. Lamberti (2023), *Libertà di informazione, poteri privati e tutela dei dati personali nell'era digitale*, in "Dirittifondamentali.it", 2023, n. 3

M. Hellmeier, F. von Scherenberg (2023), *A Delimitation of Data Sovereignty from Digital and Technological Sovereignty*, in ECIS Research Papers, 2023

J. Henni (2015), *Les résultats catastrophiques du cloud à la française*, BFM Business, 26 mai 2015

F. Hilgert (2015), *Das IT-Sicherheitsgesetz: Neue Anforderungen für alle geschäftsmäßigen Onlinedienste*, in "CRonline.de Blog", 2015

W.K. Hon, C. Millard, J. Singh et al. (2016), *Policy, legal and regulatory implications of a Europe-only cloud*, in "International Journal of Law and Information Technology", vol. 24, 2016, n. 3

P. Hummel, M. Braun, M. Tretter, P. Dabrock (2021), *Data sovereignty: A review*, in "Big Data & Society", 2021

Institut d'Histoire de l'Industrie (1998), *Informatique, politique industrielle, Europe: entre plan calcul et unidata*, Rive Droite, 1998

L. Lessig (2006), *Code: And Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006

L. Lessig (1999), *Code and Other Laws of Cyberspace*, Basic Books, 1999

G.M. Lombardi (1970), *Potere privato e diritti fondamentali*, Giappichelli, 1970

M.E. Macron (2018), *Speech by M. Emmanuel Macron, President of the Republic at the Internet Governance Forum*, 12 November 2018

B. Mirkine-Guetzévitch (1933), *Droit Constitutionnel International*, Librairie du Recueil Sirey, 1933

N. Mishra (2015), *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?*, in SSRN, 2015

F. Misterek (2017), *Digitale Souveränität Technikutopien und Gestaltungsansprüche demokratischer Politik*, MPIfG Discussion Paper, 2017

M.A. Montebourg (2013), *Déclaration de M. Arnaud Montebourg, ministre du redressement industriel, sur les 34 plans de la nouvelle France industrielle, au Massachussetts Institute of Technology (MIT)*, 18 novembre 2013

M. Monti (2019), *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in "Rivista italiana di informatica e diritto", 2019, n. 1

E. Mostacci (2008), *La soft law nel sistema delle fonti: uno studio comparato*, Cedam, 2008

P. Mouron (2024), *La loi visant à sécuriser et réguler l'espace numérique est promulguée. Revue européenne des médias et du numérique*, in HAL science ouverte, 2024

M.L. Mueller (2020), *Against Sovereignty in Cyberspace*, in "International Studies Review", 2020, n. 4

B. Pastore (2003), Soft law*, gradi di normatività, teoria delle fonti*, in "Lavoro e diritto", 2003

I. Pernice (2016), *Global Constitutionalism and the Internet. Taking People Seriously*, in S. Kadelbach, R. Hofmann (eds.), "Law Beyond the State. Pasts and Futures", Campus Verlag, 2016

J. Pohle (2020), *Digital sovereignty. A new key concept of digital policy in Germany and Europe*, Konrad-Adenauer-Stiftung, 2020

J. Pohle, T. Thorsten (2021), *Digitale Souveränität. Von der Karriere eines einenden und doch problematischen Konzepts*, in. C. Piallat (hg.), "Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt", transcript Verlag, 2021

O. Pollicino (2023), *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in "Quaderni costituzionali", 2023, n. 3

O. Pollicino (2018), *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in V. Piccone, O. Pollicino (a cura di), "La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività", Editoriale Scientifica, 2018

Presidenza tedesca del Consiglio dell'Unione europea (2020), *Expanding the EU's digital sovereignty*, 2020

U.K. Preuss (2010), *Disconnecting Constitutions from Statehood: Is Global Constitutionalism a Viable Concept?*, in P. Dobner, M. Loughlin (eds.), "The Twilight of Constitutionalism?", Oxford University Press, 2010

S. Rodotà (2014) *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014

S. Rodotà (2012) *Il diritto di avere diritti*, Laterza, 2012

S. Rodotà (2010), *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3

S. Rodotà (1997), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, 1997

A. Sajó (1999), *Limiting Government: An Introduction to Constitutionalism*, Central European University Press, 1999

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1

M. Santaniello, N. Palladino, M.C. Catone, P. Diana (2018), *The Language of Digital Constitutionalismand the Role of National Parliaments*, in "International Communication Gazette", vol. 80, 2018, n. 4

A. Somma (2008), *Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti*, in "Rivista critica del diritto privato", 2008, n. 3

C. Spiniello (2022), *Formazione (e crisi) dei Governi: il ruolo del Presidente della Repubblica. Verso un correttivo presidenziale della forma di governo parlamentare italiana*, in D. Paris (a cura di), "Il primo mandato di Sergio Mattarella. La prassi presidenziale tra continuità ed evoluzione", Editoriale Scientifica, 2022

C. Spiniello (2018), *(Sche)Dati. Il diritto alla protezione dei dati personali nella legislazione europea*, in "Democrazia e Sicurezza – Democracy and Security Review", 2018, n. 1

G. Teubner (2012), *Constitutional Fragments: Societal Constitutionalism and Globalization*, Oxford University Press, 2012

G. Teubner (2004), *Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?*, in C. Joerges, I.-J. Sand, G. Teubner (eds.), "Transnational Governance and Constitutionalism", Hart Publishing, 2004

G. Vasino (2023), *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in "federalismi.it", 2023, n. 4

G. Zagrebelsky (1981), *La Corte costituzionale e il legislatore*, in "Il Foro italiano", 1981, n. 10

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0208 • articolo sottoposto a peer review • pubblicato in anteprima il 19 mag. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Dario Saul Navarro – José Osvaldo Ledesma

Inteligencia artificial generativa aplicada a la valoración probatoria en un caso de prescripción adquisitiva

El presente artículo analiza el rendimiento de una herramienta de inteligencia artificial generativa como asistente para la valoración de pruebas en un proceso de prescripción adquisitiva, al que se suministraron pruebas de un caso real. Este análisis se basa en un registro de experimentos realizados con una herramienta disponible en ChatGPT-4o, conocida como "Custom GPT" o "GPT personalizados", que se diseñó con técnicas de ingeniería de prompts adaptadas a esta tarea jurídica compleja. Como resultado, se concluye que este GPT puede funcionar como un asistente útil, capaz de integrar las distintas pruebas bajo los principios de la sana crítica racional, aunque su efectividad estará condicionada en último término por la intervención y el control humano.

Ingeniería de prompts – Justicia digital – Derecho procesal – Sana crítica racional

Generative artificial intelligence applied to evidence evaluation in an acquisitive prescription case

This article analyzes the performance of generative artificial intelligence as an assistant for evidence evaluation in an acquisitive prescription process, where real case evidence was provided. This analysis is based on a record of experiments conducted with a tool available in ChatGPT-4o, known as "Custom GPT", designed with prompt engineering techniques tailored to this complex legal task. As a result, it is concluded that this GPT can function as a useful assistant, capable of integrating various pieces of evidence under the principles of rational critical analysis. However, its effectiveness ultimately depends on human intervention and oversight.

Prompt engineering – Digital justice – Procedural law – Rational critical analysis

D.S. Navarro es investigador en la Facultad de Derecho y ciencias sociales y políticas de la Universidad Nacional del Nordeste, Argentina

J.O. Ledesma es profesor libre de Derecho procesal civil, Cátedra B, en la Facultad de Derecho y ciencias sociales y políticas de la Universidad Nacional del Nordeste, Argentina

Resumen: 1. Introducción. – 1.1. Problema e hipótesis. – 1.2. Metodología. – 2. El proceso de prescripción adquisitiva en el Código Civil y Comercial argentino. – 2.1. La prescripción adquisitiva o usucapión. – 2.2. Posesión requerida para usucapir. – 2.3. La prueba en procesos de prescripción adquisitiva. – 3. Inteligencia artificial generativa y valoración probatoria. – 3.1. Caracterización de los Grandes Modelos de Lenguaje. – 3.2. Potencialidades y limitaciones de los grandes modelos de lenguaje en la valoración probatoria. – 4. Diseño del GPT adaptado a la valoración probatoria mediante ingeniería de prompt. – 4.1. Los GPTs personalizados. – 4.2. Ingeniería de prompts aplicada al diseño del GPT. – 4.3. Instrucciones suministradas. – 5. Análisis de los resultados obtenido. – 5.1. El caso suministrado. – 5.2. Cumplimiento de las instrucciones introducidas al GPT. – 5.3. Calidad de las respuestas. – 5.4. Análisis individual de las pruebas. – 5.5. Indicadores de rendimiento. – 6. Especificidad del caso y exportabilidad de los resultados. – 7. Conclusión.

1. Introducción

A partir del lanzamiento de ChatGPT 3.5 por la empresa OpenAI, la inteligencia artificial generativa (IAGen) ha impactado al mundo por su capacidad para procesar y generar lenguaje natural. Estos modelos informáticos han logrado realizar actividades que hasta hace pocos años se consideraban exclusivas de la inteligencia humana, tales como redactar poemas, resolver exámenes académicos o interpretar textos.

Las posibilidades de lo que podemos solicitarle a ChatGPT parecen ser infinitas, como también lo son sus usos[1]. Pero también hay voces que afirman que el conjunto de tecnologías englobadas en el paradigma de IA no deberían tomarse ni con fanatismos a favor, ni con fetichismos en contra[2].

Ante este escenario plagado de incertidumbres y posibilidades, la aplicación de esta tecnología para tareas de razonamiento jurídico complejo todavía no se encuentra suficientemente examinada por la doctrina, y se registra un uso incipiente en la práctica judicial.

En base a esta situación, el presente artículo se enfoca en evaluar la capacidad operativa de una herramienta provista por ChatGPT, denominada "Custom GPT" o "GPT personalizado", para ser empleada como asistente en la valoración probatoria de los procesos de prescripción adquisitiva en Argentina.

La elección del proceso de prescripción adquisitiva se justifica porque se producen distintos tipos de medios probatorios (documental, testimonial, pericial, etc.), lo que permitirá evaluar el grado de adaptación del GPT a distintos escenarios. Esto mismo, además, podría brindar elementos para considerar una eventual extrapolación a otros tipos de procesos, en los que prime el principio de amplitud probatoria.

1.1. Problema e hipótesis

Para la doctrina procesalista tradicional, la valoración de la prueba es el análisis crítico e integral del conjunto de elementos de convicción reunidos y definitivamente introducidos en el proceso,

1. García Sánchez 2023.
2. Álvarez Saez 2023.

poniéndose énfasis en que se trata de un razonamiento lógico-valorativo[3].

Este enfoque de la valoración probatoria encuentra su manifestación más palmaria en el sistema denominado "sana crítica racional". Couture[4] lo define como las reglas del correcto entendimiento humano, contingentes y variables en relación con la experiencia del tiempo y lugar, pero estables y permanentes en cuanto a los principios lógicos en que debe apoyarse la sentencia.

De estas caracterizaciones surge que la valoración probatoria en general, y la sana crítica en especial, están esencialmente unidas a la inteligencia humana. En efecto, la sana crítica racional no solo implica el uso de la razón, sino también de la experiencia cotidiana como parámetro de ajuste al caso concreto.

Ahora bien, Corvalán y Carro[5] señalan que la limitación central de la IAGen es que solo registra los datos en términos de código y realiza correlaciones estadísticas, pero no tiene una comprensión del mundo real y carece de la capacidad de representar los datos en forma conceptual.

En este marco, surge el interrogante ¿Un GPT personalizado puede hacer valoraciones propias de la sana crítica racional si se le suministran pruebas de un caso real de prescripción adquisitiva?

Para abordar este problema, se ha elaborado la siguiente hipótesis: "*Un GPT personalizado, cuando se le solicita que valore las pruebas producidas en un caso real, puede generar conclusiones dentro de los parámetros de la sana crítica*".

Esto es así por cuanto, a nivel conjetural, se estima que la IAGen tiene el potencial necesario para valorar pruebas emulando una actividad intelectual humana de alto nivel, tal como es la que se realiza en el marco de la sana crítica racional.

1.2. Metodología

Para verificar esta hipótesis, se aplicó una metodología experimental con un enfoque de evaluación cualitativa. Para realizar los tests, se desarrolló un GPT al que se introdujeron instrucciones para valorar prueba siguiendo las reglas de la sana crítica racional, junto a criterios especiales de valoración probatoria para casos de prescripción adquisitiva.

Para realizar la comprobación empírica, se tomó como insumo el acervo probatorio producido en un expediente real de prescripción adquisitiva. Para preservar la privacidad de los justiciables, se procedió al cifrado de los datos personales y registrales.

Para verificar la consistencia de las respuestas, en total se realizaron cinco tests, cuyos resultados fueron registrados en una planilla[6]. En cada prueba se analizó la calidad del análisis probatorio, la estructura de la respuesta dada por la IAGen, la extensión y calidad de las conclusiones parciales y finales, así como otros comentarios adicionales.

2. El proceso de prescripción adquisitiva en el Código Civil y Comercial argentino

2.1. La prescripción adquisitiva o usucapión

El Código Civil y Comercial de la Nación en su art. 1897 dispone que: "La prescripción para adquirir es el modo por el cual el poseedor de una cosa adquiere un derecho real sobre ella, mediante la posesión por el tiempo fijado por la ley". En la práctica, comúnmente los procesos de prescripción adquisitiva de inmuebles se fundan en la posesión sin justo título ni buena fe. Para este tipo de casos, el art. 1899 del mismo Código establece que: "Si no existe justo título y buena fe, el plazo es de veinte años. No puede invocarse contra el adquirente la falta o nulidad del título o de su inscripción, ni la mala fe de su posesión".

2.2. Posesión requerida para usucapir

Conforme lo establece el art. 1909 del Código Civil y Comercial de la Nación, existe posesión "cuando una persona, por sí o por medio de otra, ejerce un poder de hecho sobre una cosa, comportándose como titular de un derecho real, lo sea o no".

De esta definición legal se desprenden sus dos elementos: uno objetivo, el *corpus* (cuerpo), que es la tenencia material de la cosa y otro subjetivo, el *animus domini* (ánimo de dueño), que implica

3. Quadri 2011.
4. Couture 1978.
5. Corvalán–Carro 2023.
6. *Registro de pruebas ChatGPT*.

la creencia efectiva de que se es propietario de la cosa. Pero este elemento subjetivo no está solo en la mente del poseedor, sino que debe exteriorizarse a través de actos ostensibles (visibles por todos) que demuestren esa verdadera intención, de otro modo, si solo fuera un estado anímico, sería imposible demostrarlo y diferenciar la "posesión" de la "simple tenencia"[7].

2.2.1. Requisitos específicos de la posesión

Sin perjuicio de lo anterior, la posesión también debe reunir los siguientes requisitos:

2.2.1.1 Pública. El art. 1900 del Código Civil y Comercial de la Nación establece que la posesión para adquirir debe ser ostensible. Esto quiere decir, que sea conocida por todos, en oposición a la que es ejercida en forma clandestina.

2.2.1.2 Continua. El citado artículo 1900 también establece expresamente la continuidad de la posesión como requisito para prescribir. Esto implica que se ejerza, en principio, sin intermitencias o lagunas, pero su aplicación concreta va a depender de la naturaleza de la cosa poseída y las circunstancias del caso.

2.2.1.3 Pacífica. Junto al carácter ininterrumpido de la posesión, se trata de exigencias no enumeradas por el art. 1900 pero sobre cuya necesidad de verificación para la procedencia de la acción, la doctrina es unánime[8]. Asimismo, se ha señalado que "la posesión de cosas poseídas por fuerza o con violencia, no comienza sino el día que se hubiese purgado el vicio"[9].

2.2.1.4 Ininterrumpida. La interrupción de la prescripción puede ser natural (lo que se da por el despojo) o civil[10] (la que se produce por demanda promovida por el propietario, juicio de árbitros o reconocimiento por parte del poseedor). Su concreción significa el comienzo de una nueva posesión sin importar todo el tiempo transcurrido con anterioridad.

2.3. La prueba en procesos de prescripción adquisitiva

La prescripción adquisitiva tiene como efecto la declaración judicial de la extinción de un derecho de propiedad sobre un inmueble y hacer nacer otro en su reemplazo. Por lo tanto, el deber general del juez de valorar el material probatorio a la luz de la sana crítica es mucho más estricto que en otros asuntos. La comprobación de la posesión en los términos legales debe ser clara y convincente, asegurando así el título que se va a obtener[11].

2.3.1. Particularidades probatorias

2.3.1.1 Prueba compuesta. Según el art. 24 inc. c) de la ley N° 14.159: "Se admitirá toda clase de pruebas, pero el fallo no podrá basarse exclusivamente en la testimonial". A partir de esta norma, la doctrina habla de la necesidad de constatar la existencia de "prueba compuesta", entendida como aquella que surge de la concordancia y convergencia entre las distintas evidencias aunque, tomadas aisladamente, no abarquen todos los pormenores del hecho[12].

2.3.1.2 Inicio de la posesión. Para determinar si ha transcurrido el lapso requerido para la adquisición del dominio, resulta esencial acreditar cuando inició. Además, resulta imperativo acreditar el ingreso al inmueble en carácter de propietario, ya que su ocupación puede obedecer a distintas razones y no todas tienen la misma consecuencia en relación a la prescripción adquisitiva[13].

7. Causse–Pettis 2015, p. 41.
8. Bueres 2014.
9. Smayevsky 2007, p. 137.
10. En este sentido, el artículo 2546 del Código Civil y Comercial de la Nación dispone: "El curso de la prescripción se interrumpe por toda petición del titular del derecho ante autoridad judicial que traduce la intención de no abandonarlo, contra el poseedor, su representante en la posesión, o el deudor, aunque sea defectuosa, realizada por persona incapaz, ante tribunal incompetente, o en el plazo de gracia previsto en el ordenamiento procesal aplicable".
11. Flah–Smayevsky 1987.
12. Quadri 2011.
13. Superior Tribunal de Justicia, Expediente Nº EXP -88715/13, "Ramirez Victoriano c/ sucesion de Camnasio Eduardo José y Azar José Luis s/ prescripcion adquisitiva - ordinario", sentencia N° 25/2024.

2.3.1.3 Pago de impuestos. De acuerdo al ya mencionado inc. c) de la ley N° 14.159: "Será especialmente considerado el pago, por parte del poseedor, de impuestos o tasas que graven el inmueble, aunque los recibos no figuren a nombre de quien invoca la posesión". Sin embargo, la jurisprudencia sujeta la relevancia del pago de impuestos a la periodicidad de su erogación durante el transcurso del plazo de prescripción adquisitiva. En rigor, no es lo mismo abonar los impuestos correspondientes a 20 años de una sola vez, que el pago frecuente y sostenido en distintas oportunidades a lo largo de los años[14].

3. Inteligencia artificial generativa y valoración probatoria

3.1. Caracterización de los Grandes Modelos de Lenguaje

La revolución de la IAGen está motorizada por los denominados "Grandes Modelos de Lenguaje" o "*Large Language Models*" (LLM), que constituyen la arquitectura informática que permiten el funcionamiento de aplicaciones como ChatGPT (desarrollada por OpenAI), Gemini (desarrollada por Alphabet, empresa matriz de Google) o Copilot (creada por Microsoft), entre otras.

La tecnología subyacente a los LLM se denomina "inteligencia artificial generativa" (IAGen) debido a que pueden producir nueva información, previamente no vista, dependiente de los datos con los que fueron entrenados. Estos modelos están desarrollando contenido fresco, similar al creado por humanos[15].

Los LLM son programas de propósito general con la capacidad de generar texto coherente y relevante para una multitud de tareas empleando el lenguaje natural, en lugar de estar capacitados para una tarea específica, como el análisis de sentimientos, el reconocimiento de entidades nombradas o el razonamiento matemático[16]. Para capturar esta versatilidad, la Ley de IA de la Unión Europea clasifica estos sistemas como inteligencia artificial (IA) de propósito general o modelos fundacionales[17].

Aunque no están diseñados para realizar tareas propias del campo jurídico, su versatilidad en el manejo del lenguaje le permite responder preguntas abiertas, analizar textos o redactar documentos completos[18]. Al examinar la vinculación entre esta tecnología y el ámbito legal, Ma et al.[19] apuntan que el lenguaje jurídico está encapsulado en el lenguaje natural, de modo que en principio, los LLM son capaces de emular el flujo de trabajo jurídico. Esta versatilidad abre un abanico de nuevas posibilidades en el campo jurídico, así como múltiples desafíos y riesgos[20].

3.2. Potencialidades y limitaciones de los grandes modelos de lenguaje en la valoración probatoria

Los sistemas de justicia atraviesan un proceso de transformación donde la IA se presenta como una herramienta promisoria para la optimización de la valoración probatoria. La integración de esta tecnología en el proceso busca aumentar la eficiencia, precisión y transparencia en el análisis de las pruebas, automatizando tareas repetitivas y facilitando el acceso a la justicia, con el debido respeto a las garantías procesales[21].

En punto a la prueba documental y de informes, la IAGen organiza los datos, estructura la información detecta patrones e identifica inconsistencias, incoherencias y contradicciones.

Con respecto a la prueba testimonial y confesional, conocidas como pruebas de interrogatorio, los LLM pueden llevar a cabo una muy buena *performance*. Según Nieva (2010, citado por Martínez Nicholls y Marroquín, 2024, p. 33), la valoración de este tipo de pruebas debe prestar atención a

14. Tribunal: Cámara de Apelaciones en lo Civil y Comercial de Santa Fe. III. Vázquez Martha Noemí y otros c/ Gamboa Antonio Cayetano y otros s/ usucapión. 5-jul-2019 Cita: MJ-JU-M-121429-AR | MJJ121429.
15. García-Peñalvo–Vázquez-Ingelmo 2023, p. 7.
16. Wei–Tay–Bommasani et al. 2022.
17. Contini 2024.
18. OpenAI, Text generation models.
19. Ma–Sinha–Tandon–Richards 2024.
20. Corvalán–Sánchez Caparrós 2023.
21. Martínez Nicholls–Marroquín 2024.

los siguientes elementos: (i) la coherencia de la declaración, (ii) el contexto, (iii) la corroboración y concordancia con demás medios de prueba para evitar inconsistencias y, (iv) las declaraciones innecesarias. Pues bien, con la configuración y prompts adecuados, los LLM tienen la potencialidad de identificar y exponer los cuatro elementos de manera satisfactoria. Además, se dice que es posible desarrollar un algoritmo que incorpore principios de psicología del testimonio para analizar la veracidad de las declaraciones[22].

En relación con la prueba pericial, la IAGen puede detectar solidez en los argumentos, inconsistencias y contradicciones, así como también, rigor lógico y metodológico empleado en los dictámenes. De igual modo, puede efectuar sugerencias disciplinares específicas, lo cual no es aconsejable por cuanto el juzgador no es un experto en la materia y podría carecer de la capacidad para valorar críticamente o rebatir los argumentos del perito desde un enfoque estrictamente técnico.

En lo que respecta al reconocimiento judicial, al suministrar el acta correspondiente, la IAGen podría generar conclusiones fundamentadas, examinando puntos clave y realizando conexiones entre la prueba y las postulaciones básicas y detectando posibles inconsistencias en el caso.

Si bien las ventajas apuntadas son significativas, no se pueden soslayar las limitaciones generales de los LLM, las cuales afectan cualquier tarea y, en particular, a la valoración probatoria. Estas tecnologías presentan un desafío importante debido a las llamadas "alucinaciones", que son respuestas que parecen coherentes y plausibles, pero que son incorrectas, por carecer de base factual sólida o por reproducir datos de entrenamiento sesgados, vale decir, contaminados con estereotipos o prejuicios. Sin dudas, analizar pruebas con este prisma puede llevar a conclusiones equivocadas, sin una adecuada revisión crítica por parte del juzgador.

Otro problema relevante es la falta de transparencia de estos sistemas, conocidos como "cajas negras", por cuanto no permiten realizar una adecuada trazabilidad entre las entradas y salidas, así como el control del manejo de los datos procesados.

En lo que a valoración probatoria en general se refiere, sin perjuicio de lo que se expondrá en líneas siguientes respecto del caso de la prescripción adquisitiva, la IAGen de uso general suele quedarse a mitad de camino, pues si bien sigue reglas de la lógica, no tiene experiencia humana ni sentido común, elementos esenciales de la sana crítica racional, problema que no existe en sistemas legales o tasados, donde la ley asigna un peso probatorio específico a cada elemento[23].

Estas carencias pueden mitigarse en gran medida mediante la personalización o ajuste fino. También es posible, aunque más difícil, trasladar el proceso de valoración probatoria al ámbito algorítmico, es decir, el del entrenamiento principal, lo cual requiere que su programación se fundamente en garantías jurídicas y derechos fundamentales de acuerdo a las leyes vigentes[24].

4. Diseño del GPT adaptado a la valoración probatoria mediante ingeniería de prompts

4.1. Los GPTs personalizados

La versión ChatGPT-4o, desarrollada por la empresa OpenAI, ofrece la posibilidad de adaptar el LLM para usos específicos, mediante una aplicación denominada "Custom GPTs" o "GPTs personalizados"[25]. Los GPTs personalizados pueden configurarse con información específica de un dominio o tarea sin conocimientos en programación, lo que democratiza la generación de aplicaciones ajustadas a necesidades particulares.

La ventaja de diseñar un GPT consiste en ofrecer respuestas ajustadas a un campo disciplinar en particular, con un tono y estilo determinados, lo que le da mayor precisión a sus respuestas y disminuye el riesgo de alucinaciones. La clave del éxito de un GPT reposa en un adecuado empleo de estrategias y tácticas de ingeniería de prompts,

22. Vilchis Robles 2024.
23. *Ibidem*.
24. Martínez Nicholls–Marroquín 2024.
25. Para crear los GPTs personalizados es necesario adherirse a una suscripción paga, no obstante, los usuarios gratuitos pueden hacer uso de los modelos creados por otros usuarios.

para elaborar la configuración inicial. Esto implica una adecuada descripción de las tareas que debe llevar a cabo, así como lo que se espera de él (lo que se conoce como *system prompt*) y un adecuado suministro de reglas de inferencias para guiar la formulación de output o respuestas. Además, el sistema permite formar una base de conocimiento en la que se pueden subir hasta 20 archivos y el formato aconsejable es de texto (txt o similar), tratando de evitar pdf o ppt. Si contuviera imágenes, éstas simplemente serán soslayadas[26].

4.2. Ingeniería de prompts aplicada al diseño del GPT

La ingeniería de prompts abarca una amplia gama de estrategias y técnicas para la elaboración de instrucciones que se ingresan a un LLM con el fin de aumentar la calidad y relevancia de sus respuestas[27]. Para el diseño de este GPT se utilizaron técnicas de ingeniería de prompts con el fin de que sea capaz de valorar pruebas en un proceso de prescripción adquisitiva, bajo los principios de la sana crítica racional.

Para emular una tarea compleja, como el razonamiento de un juez, resulta necesario que las instrucciones se formulen de forma metódica y sistemática. Por ello, la técnica que rigió la elaboración de las instrucciones del GPT fue el de cadena de pensamientos ("Chain of Thought" o CoT), introducido por Wei et al.[28]. El CoT permite a los LLM resolver un problema como una serie de pasos intermedios que imitan un proceso de pensamiento antes de dar una respuesta final. Esta técnica se utiliza para tareas que requieren que un humano piense detenidamente, como matemáticas complejas, análisis de varios pasos, redacción de documentos complejos o decisiones con múltiples factores[29].

La ingeniería de prompts se concentró en la elaboración de instrucciones del GPT, de manera que pueda asumir un rol de evaluador de pruebas bajo los estándares de la sana crítica racional. Esto permitió que el contenido de las distintas pruebas del proceso se ingrese de forma directa, sin necesidad de aclaraciones de contexto. Asimismo, el suministro del plexo probatorio se efectuó en prompts separados, según el contenido de cada prueba. De este modo, por ejemplo, en un prompt se ingresó el contenido de un boleto de compraventa, y en otro prompt, un acta de reconocimiento judicial realizado sobre el inmueble objeto del proceso.

4.3. Instrucciones suministradas

Para aumentar la eficiencia del modelo, se asignó el objetivo específico de "Analizar pruebas para determinar si se ha demostrado la posesión de un inmueble por un período de al menos 20 años a la fecha de promoción de la demanda". Al mismo tiempo, se le instruyó para no responder preguntas que no respondan a ese objetivo.

Se asignó al GPT el rol de juez especialista en derecho civil argentino. Se le indicó que se exprese en un tono "formal y claro, utilizando jerga jurídica sólo cuando sea necesario".

4.3.1. Criterios jurídicos

Para ajustar el rendimiento a los resultados esperados, se explicitaron los criterios jurídicos aplicables. Se dividieron los criterios jurídicos en tres apartados distintos: la determinación de los elementos de la posesión, criterios generales de valoración jurídica y criterios especiales de valoración de distintos tipos de pruebas.

4.3.1.1 Elementos de la posesión. Se indicaron los elementos de la posesión para prescribir un inmueble en los términos del Código Civil y Comercial de la Nación Argentina. Estos son: *Corpus*: Capacidad material de disponer de la cosa. *Animus domini*: Actuar como dueño sin reconocer la propiedad en otro. Plazo mínimo: 20 años. Características: Pública, pacífica, continua e ininterrumpida[30].

26. Pardo 2024.
27. OpenAI, Prompt engineering.
28. Wei–Wang–Schuurmans et al. 2022.
29. V. el sitio web Anthropic.
30. Elementos de la posesión: *Corpus*: Capacidad material del poseedor de disponer de la cosa como quiera, impidiendo toda injerencia ajena. *Animus domini*: El poseedor debe actuar como dueño y no reconocer en otro la propiedad. Plazo mínimo: 20 años. Características de la posesión: Pública: Debe ser conocida por terceros.

4.3.1.2 Criterios generales de valoración probatoria. Se brindaron pautas generales para la evaluación de la prueba. Se instruyó al modelo para que haga uso de la lógica y máximas de la experiencia humana (sana crítica racional). Se le requirió un análisis individual paso a paso de cada prueba. Finalmente, se le indicó que debía integrar las valoraciones parciales de cada prueba en una consideración global antes de emitir una conclusión[31].

4.3.1.3 Criterios especiales por tipo de prueba. Se sintetizaron en reglas concretas y literales, distintos criterios jurisprudenciales y doctrinarios aplicables a procesos de prescripción adquisitiva. A modo de ejemplo, las reglas de valoración específicas incluidas fueron la preferencia por documentos públicos o privados con firma certificada o la valoración preferente de comprobantes de pago de impuestos y servicios.

4.3.1.4. Proceso de interacción. La forma en que se suministran los datos al GPT puede condicionar en gran parte la efectividad de la labor de la IA. Para ordenar este proceso, se brindaron instrucciones específicas. En primer lugar, se generó un iniciador de conversación que indica al usuario a hacer click en un botón determinado. Una vez que el usuario ingresa, el proceso de interacción se estructura en cuatro fases principales:

1. Solicitud de información inicial: El modelo solicita datos sobre los actores, la fecha de presentación de la demanda y un resumen de los hechos relevantes.
2. Recopilación de pruebas: El modelo solicita al usuario que ingrese las pruebas una por una, clasificándolas en categorías como documental, informativa, testimonial, reconocimiento judicial y otras.
3. Evaluación de pruebas: A medida que se ingresan las pruebas, el modelo las compara con los hechos de la demanda y con las pruebas anteriores, realizando conclusiones parciales.
4. Evaluación final y línea de tiempo: Tras analizar todas las pruebas, el modelo realiza una evaluación conjunta y concluye si se ha demostrado la posesión alegada. A pedido del usuario, puede elaborar una línea de tiempo con los hitos fundamentales de la posesión.

5. Análisis de los resultados obtenidos

El estudio experimental se basó en la realización de cinco tests diseñados para evaluar el rendimiento del modelo GPT. En cada test, se introdujo, de manera separada y en el mismo orden, el contenido de diversas evaluaciones correspondientes a un caso real de prescripción adquisitiva.

5.1. El caso suministrado

M.L y V.P promovieron una demanda de prescripción adquisitiva de dominio respecto a un inmueble ubicado en la localidad de Berón de Astrada, provincia de Corrientes, República Argentina. Manifestaron que se encuentran casados desde 1966 y que establecieron el hogar familiar en el inmueble objeto de la demanda. Refieren que el 22 de septiembre de 1988 celebraron un Boleto de Compraventa entre los herederos del Sr. A. I. M. y la Sra. M. L. por dicho inmueble.

Alegan que el inmueble tiene una menor extensión que la que figura en el Registro de la propiedad, debido a que la propiedad original fue objeto de distintas subdivisiones a lo largo del tiempo. Para demostrar los antecedentes del inmueble, presentaron tres planos de mensura y un convenio de delimitación de terrenos.

Además, sostienen que han pagado regularmente impuestos desde 2002 hasta 2020, y han presentado numerosos recibos de pago. Asimismo, refieren que su posesión es ampliamente conocida por los vecinos de la localidad y ofrecieron la declaración de tres testigos.

Pacífica: Sin violencia. Si comenzó con un vicio, debe purgarlo antes de que se cuente el tiempo de posesión pacífica. Continua: Debe ser constante, sin interrupciones. Ininterrumpida: Sin despojos ni demandas que corten el plazo.

31. Criterios de valoración probatoria: Usaré la lógica y las máximas de la experiencia humana (sana crítica racional). Analizaré las pruebas individualmente y en conjunto, buscando correlaciones o discrepancias para verificar la posesión. Evaluaré cada prueba paso a paso para asegurarme de dar una respuesta correcta. El orden en que se suministran las pruebas no es relevante. No me apresuraré a dar una respuesta hasta que haya analizado todas las pruebas de forma global.

Los demandados fueron los propietarios registrales, quienes no se presentaron al proceso. Por lo tanto, no se presentaron pruebas que contrarresten la postura de los actores.

En este caso, la dificultad para el GPT consiste en valorar de forma ordenada una amplia cantidad de distintos tipos de pruebas[32], relacionándolas de forma coherente bajo los distintos parámetros legales que se exigen en la prescripción adquisitiva. En particular, la principal dificultad estaba dada en dilucidar el historial registral del inmueble.

5.2. Cumplimiento de las instrucciones introducidas al GPT

En la mayoría de los casos el GPT siguió las pautas de interacción con el usuario. Sin embargo, en un par de tests, cuando se habían suministrado la mayoría de las pruebas se adelantaba a ofrecer conclusiones finales a pesar de que todavía no se le había indicado que realice su conclusión. De todas formas, esas conclusiones anticipadas eran muy escuetas y superficiales; carecían de la riqueza y calidad de análisis que luego mostraban las conclusiones finales, en las que sí realizaba una valoración probatoria integral.

Por otro lado, el GPT evidenció un rendimiento consistente en el seguimiento de las reglas de valoración probatoria, brindando resultados similares en cada uno de los tests.

5.3. Calidad de las respuestas

En los 5 test realizados, el GPT exhibió un rendimiento consistentemente alto y en su evaluación final, recomendó hacer lugar a la demanda de prescripción (tab. 1).

En los distintos test el GPT comprendió que el inmueble objeto de la prescripción se trataba de un lote que había sido objeto de sucesivas subdivisiones en el pasado. Además, determinó con certeza el inicio de la posesión, en base a la fecha de celebración del boleto de compraventa del inmueble. Vale destacar que en los test 3 y 5, al valorar los

Test	Calidad de respuestas	Evaluación final integral
1)	4	Estructura bien organizada con resumen de hechos, análisis de pruebas, evaluación de posesión y conclusión final a favor de admitir la demanda.
2)	4	Conclusión final realizada sin orden expresa. Análisis desde 4 aristas: *corpus*, *animus domini*, características de la posesión y estado registral. Conclusión a favor de admitir la demanda, aunque un poco escueta.
3)	4	Estructura similar al primer test, pero omite la evaluación de la posesión en relación con los requisitos legales. Análisis individual de pruebas algo escueto. Conclusión muy buena.
4)	4	Estructura con resumen del caso, análisis de elementos de posesión, conclusión final y apartado de "decisión". Usa lenguaje claro. No analiza todas las pruebas, sólo las relevantes para los puntos mencionados.
5)	4	Muy bueno. Análisis dividido por tipos de pruebas. Incluye conclusión final y "propuesta final" indicando cómo debería ser la sentencia. Pequeño error en el adrema actual del inmueble.
Escala: 1= Deficiente; 2= Baja; 3=Media, 4= Alta; 5= Excelente		

Tab. 1 — *Tabla de calidad de respuestas y evaluación final integral en cada test*

32. Como prueba documental se presentaron 3 planos de mensura, 3 certificados de libre deuda inmobiliario, 2 certificados de valuación fiscal, libreta de familia, boleto de compraventa, convenio de delimitación de terrenos y 15 comprobantes de pago de impuesto inmobiliario. Además se produjeron 3 declaraciones testimoniales, un reconocimiento judicial registrado en un acta y 6 fotografías; un informe del Registro Municipal y otro informe del Registro de la Propiedad Inmueble.

recibos de pago de impuestos, apreció que esto se corresponde al *animus* de la posesión, tal como lo precisa la doctrina[33]. Sin embargo, en el test 2 también lo identificó con el *corpus*[34], lo cual contraría las máximas de la experiencia, ya que no es necesario ocupar el inmueble para pagar los impuestos.

Por otro lado, el GPT evaluó de forma conjunta las distintas declaraciones testimoniales, y evaluó su grado de parcialidad y el conocimiento directo que adujeron haber tenido sobre los hechos que declararon.

Por último, en la mayoría de los tests, en principio, no se detectaron alucinaciones ni afirmaciones contrarias al ordenamiento jurídico vigente ni a la lógica y experiencia humanas[35].

Test	Conclusiones parciales en cada prueba
1)	A1-A5: Muy bueno/Bueno. A6-A8: Bueno. A9: Bueno. A10-A12: Muy bueno. B: Medio. C: Medio. D: Bueno.
2)	A1: Bueno. A2-A3: Muy bueno. A4: Bueno. A5: Muy bueno. A6-A8: Bueno. A9-A10: Muy bueno. A11: Bueno. A12: Muy bueno. B: Bueno. C-D: No presenta.
3)	A1-A5: Bueno. A6-A8: Medio. A9: Bueno. A10: Medio. A11-A12: Bueno. B-C: Bueno. D: Muy bueno.
4)	A1-A3: Muy bueno. A4: Muy bueno. A5: Bueno. A6-A8: Medio. A9-A11: Bueno. A12: Muy bueno. B-C: Muy bueno. D: Bueno.
5)	A1-A3: No presenta. A4: Bueno. A5: No presenta. A6-A8: No presenta. A9-A11: Bueno. A12: No presenta (en forma particular para esta prueba). B: No presenta. C: Muy bueno. D: Bueno.
Referencias: A1 = Plano de Mensura 672-Y, A2 = Plano de Mensura 172-Y, A3 = Plano de Mensura 95-Y, A4-A6 = Certificados de libre deuda inmobiliario, A7-A8 = Certificados de valuación fiscal, A9 = Libreta de familia, A10 = Boleto de compraventa, A11 = Convenio de delimitación de terrenos, A12 = Impuestos; B = Prueba Testimonial (x3); C = Prueba de Reconocimiento Judicial (acta y 6 fotografías); D = Prueba Informativa (Registro Municipal y Registro de la Propiedad Inmueble)	

Tab. 2 — *Tabla de Calidad de conclusiones parciales de cada prueba particular*

5.4. Análisis individual de las pruebas

En el análisis parcial de cada prueba, el GPT intentaba dar cumplimiento a las instrucciones suministradas en su configuración. Al ingresar el contenido de una prueba, respondía con una descripción detallada de cada una, para pasar luego a exponer su relevancia para verificar el cumplimiento de la posesión en los términos legales, teniendo en cuenta los hechos y las demás pruebas. En todos los casos en que existieron conclusiones parciales, estas eran breves, generalmente de un párrafo y estaban orientadas a confirmar o refutar, a la luz de la prueba analizada, los presupuestos de procedencia de la prescripción adquisitiva (tab. 2).

El GPT mostró un rendimiento notable para analizar la prueba documental, detallando de forma pormenorizada los distintos tipos de datos contenidos en cada documento. A modo de ejemplo, en el test 1, al evaluar la mensura 172-Y, el GPT identificó los siguientes datos: *Naturaleza, Fecha de realización, Fecha de aprobación por Catastro, Funcionario firmante, Propietarios registrados, Carácter de la mensura, Realizador de la Mensura, Comitente, Ins–cripción en Catastro y Registro de la Propiedad, División de Parcela y Detalle de las dimensiones del Lote A y B* (al cual identificó como

33. Areán 2024.

34. Al valorar un certificado de libre deuda inmobiliario afirmó: "El pago continuo de los impuestos y tasas municipales demuestra una administración constante del inmueble, lo que confirma la capacidad material de disposición del bien (corpus)".

35. Excepcionalmente, en uno de los tests afirmó que la certificación de una copia implicaba publicidad del documento; que el hecho de que sea el mismo juez quien certificó las firmas de un documento implica aceptación por las partes involucradas y que la venta del bien podría haber implicado interrupción del plazo de prescripción adquisitiva. De similar manera, en otro test el GPT sostuvo que los gravámenes podrían tener efecto interruptivo.

Número de Test	Valoración de Prueba Compuesta
1)	Aunque la mensura 95-Y no aporta pruebas directas sobre la posesión de M. L., sí establece que la Parcela 5 ya existía con sus límites claros y que luego fue subdividida en mensuras posteriores (172-Y y 672-Y) relacionadas con la misma parcela. La referencia a la mensura 95-Y en la mensura 172-Y muestra una continuidad en la identificación del inmueble y la formalización de los actos posesorios posteriores.
2)	A.1 Plano de Mensura 672-Y: Descripción del inmueble: Se detalla un polígono de 4 lados, con 16 metros de frente y 58 metros de fondo, lo que coincide con las dimensiones descritas en los hechos de la demanda.
3)	a.6. Certificado de libre deuda inmobiliario: Este certificado es relevante porque se refiere específicamente a la superficie de 850 m^2, que coincide con el lote B del plano 172-Y, el cual es objeto de la prescripción adquisitiva.
4)	a.11. Convenio de delimitación de terrenos: La fracción de terreno delimitada en este convenio es la misma que, según lo relatado por M. L. y V. P., fue vendida a través del boleto de compraventa de 1988 (prueba a.10). Esto sugiere que la delimitación acordada en 1981 sirvió de base para la posterior transacción, lo que facilita el establecimiento de una posesión clara y pacífica a partir del momento en que M. L. adquirió el inmueble.
5)	C: Testimonial: Los tres testigos ubican claramente la vivienda de M. L. y V. P. en la calle San Martín, frente al Colegio Secundario, y proporcionan descripciones coincidentes de la casa (murallas con rejas, construcción de material, color de la pintura, etc.), lo que demuestra el *corpus* o la posesión material del inmueble.
Referencias: A1 = Plano de Mensura 672-Y, A2 = Plano de Mensura 172-Y, A3 = Plano de Mensura 95-Y, A4-A6 = Certificados de libre deuda inmobiliario, A7-A8 = Certificados de valuación fiscal, A9 = Libreta de familia, A10 = Boleto de compraventa, A11 = Convenio de delimitación de terrenos, A12 = Impuestos; B = Prueba Testimonial (x3); C = Prueba de Reconocimiento Judicial (acta y 6 fotografías); D = Prueba Informativa (Registro Municipal y Registro de la Propiedad Inmueble).	

Tab. 3 — *Tabla ejemplificativa de valoración de prueba compuesta*

objeto del proceso de prescripción adquisitiva). Además, al notar que la comitente de esta mensura fue la parte actora, el GPT señaló que esto podría evidenciar su ánimo de poseer como dueña, dado que normalmente este tipo de actos corresponden a quienes ejercen control efectivo sobre el bien.

5.5. Indicadores de rendimiento

Como indicadores de la calidad de las respuestas se tuvieron en cuenta: 1) la capacidad de valorar prueba compuesta, 2) el análisis dentro de los parámetros de la sana crítica y 3) la estructura de la respuesta.

5.5.1. Prueba compuesta

El GPT demostró una buena capacidad para relacionar las pruebas entre sí y alcanzar una conclusión armónica. Esta capacidad fue más notable en la relación entre las mensuras relativas al inmueble, lo que resultaba fundamental para dilucidar el caso. En la tabla 3 se incluye la transcripción literal de algunos pasajes en que el GPT analizó las evidencias de forma conjunta.

5.5.2. Análisis dentro los parámetros de la sana crítica

Uno de los aspectos destacables es que el GPT ha logrado emitir juicios valorativos racionales y ajustados a las máximas de la experiencia. En la tabla 4, se transcriben de manera literal alguna de las afirmaciones efectuadas por el GPT al valorar en particular a cada prueba.

No obstante, se observaron dificultades en la detección de ciertos detalles en pruebas específicas que presentaban datos disímiles, como diferencias en adremas (identificadores catastrales) o de nombres de calles en los comprobantes de pago de impuestos, o diversidad de propietarios y superficies en los certificados de valuación fiscal, entre los diferentes tests.

5.5.3. Estructura de las respuestas

Se observa una estructura consistente a lo largo de los tests, que generalmente incluye descripción de la prueba, análisis de relevancia, valoración, conclusión parcial y conclusiones finales.

Sin embargo, se notaron variaciones en la presentación de la información, como el uso de viñetas en vez de texto corrido, o la inclusión o no de subtítulos específicos. En algunas respuestas, la descripción de la prueba se integraba con el análisis, en vez de realizarse por separado. Sin embargo, estas diferencias en la estructura no se trasladaron a la sustancia del contenido.

que el GPT puede gestionar la recepción de información compleja.

Como ya se ha señalado, en el diseño del GPT se incluyeron criterios jurídicos específicos, como los elementos de la posesión, criterios generales de valoración probatoria y criterios especiales según el tipo de prueba. Esta estructuración permitió al modelo ajustar su rendimiento a los resultados

N° de Test	Prueba	Análisis del GPT
1)	A2	Aunque el plano está a nombre de los propietarios A. I. M. y C. C. D. L. S. de M., el hecho de que M. L. haya sido la comitente de la mensura podría evidenciar su ánimo de poseer como dueña, dado que normalmente este tipo de actos corresponden a quienes ejercen control efectivo sobre el bien.
1)	A10	Dado que la fecha de celebración del boleto de compraventa es el 21 de septiembre de 1988 y que la posesión se entregó en ese momento, este acto marca el inicio del plazo posesorio. La posesión real y efectiva concedida a la compradora es clave, ya que indica que desde ese momento M. L. estaba en posesión del inmueble, al menos a nivel contractual.
2)	B	Todos los testigos declaran conocer a M. L. y V. P. desde su llegada a Berón de Astrada en 1987, cuando comenzaron a trabajar como profesores en el Colegio Secundario. Este dato es crucial, ya que sitúa a los actores en la localidad desde una fecha cercana al inicio del período de posesión alegado (1988).
3)	A12	Los comprobantes de pago de impuestos y los recibos totalizadores son pruebas contundentes del ejercicio constante de la posesión con "*animus domini*" por parte de V. P., en su calidad de co-actor junto a M. L.
4)	C	El inmueble está equipado con servicios básicos como energía eléctrica, agua potable, teléfono, Internet y televisión satelital. La presencia de estos servicios refuerza la idea de que la vivienda ha sido habitada de manera constante.

Referencias: A2 = Plano de Mensura 172-Y, A10 = Boleto de compraventa, A12 = Impuestos; B = Prueba Testimonial (x3); C = Prueba de Reconocimiento Judicial (acta y 6 fotografías).

Tab. 4 — *Valoración en los términos de la sana crítica*

Con respecto al tono, mantuvo una expresión profesional, pero con lenguaje en general accesible, aclarando en ocasiones el significado de términos técnicos y latinismos cuando no era posible prescindir de ellos.

6. Especificidad del caso y exportabilidad de los resultados

Estos resultados permiten afirmar que la ingeniería de prompts puede resultar eficaz para guiar a un GPT en el proceso de recepción y posterior valoración de distintos tipos de pruebas. A la par, la interacción estructurada en fases –solicitud de información inicial, recopilación de pruebas, evaluación de evidencias y conclusión final– evidencia

esperados. De manera análoga, se podrían explicitar los criterios valorativos aplicables a otros procesos, en forma de reglas concretas, asimilables por el sistema.

También resulta relevante que el GPT evidenció habilidad para analizar pruebas que no son exclusivas del proceso de prescripción adquisitiva, sino que se producen en cualquier tipo de proceso judicial, como documentales, testimoniales, periciales e informativas.

A esto se suma la capacidad para relacionar y valorar pruebas de manera conjunta, de acuerdo a los principios de la sana crítica racional. Este estándar es universalmente aplicable a los procesos judiciales, ya que con excepción de los casos de

prueba tasada, en cualquier proceso los elementos probatorios deben ser valorados con coherencia y consistencia.

En cuanto a su aplicabilidad en tribunales extranjeros, aquellos sistemas regidos por el *civil law*, que comparten con Argentina los principios generales de la prescripción adquisitiva como la necesidad de *corpus y animus domini* durante un determinado periodo de tiempo, también constituyen un terreno favorable para la exportabilidad del GPT. Esto requeriría, no obstante, la personalización o configuración de un GTP similar adaptado a los requisitos concretos y plazos establecidos por la normativa de fondo y forma del país en cuestión.

En países regidos por el *common law*, la aplicabilidad de este GPT para casos de *adverse possession* resulta menos predecible, porque es un sistema donde la valoración probatoria se sustenta en precedentes judiciales y un razonamiento más casuístico, lo que exigiría complementar el GPT con *dossiers* de jurisprudencia relevante del país en cuestión y un entrenamiento específico en actividades intelectuales propias de este sistema, como la detección de la *ratio decidendi y el obiter dictum* en cada fallo analizado. Esto requeriría, además, realizar nuevos estudios e investigaciones para adaptar el GPT a este marco y, con ello, asegurar su adecuada funcionalidad.

7. Conclusión

Como conclusión es posible afirmar que se ha cumplido la hipótesis de este trabajo, toda vez que a partir de los cinco test realizados, ha quedado demostrado que el GPT personalizado, cuando se le solicita que valore pruebas, puede generar de forma consistente conclusiones dentro de los parámetros de la sana crítica. De igual manera, es preciso señalar que para brindar una conclusión categórica sería necesario experimentar con muestras más grandes.

En cuanto al rendimiento del modelo, es destacable que en los cinco test ha demostrado capacidad para relacionar pruebas entre sí para luego verificar los hechos alegados. Por otra parte, si bien el análisis probatorio ha sido similar en cada uno de los test, lo cierto es que en ningún caso las respuestas fueron idénticas, variando en el nivel de detalle en cada interacción.

Sin perjuicio de la valoración probatoria, el GPT también ha demostrado resultar muy eficiente para desagregar los datos que surgen de las distintas pruebas, lo que puede facilitar el acto de valoración por parte del operador humano.

Aunque el GPT ha demostrado ser un asistente funcional, su efectividad estará ligada a la intervención humana. En primer lugar, el sistema depende de los datos suministrados por el usuario, quien de manera previa deberá determinar su relevancia. Además, aunque el GPT emite respuestas detalladas, el usuario deberá identificar aquellos aspectos que le resulten rescatables. Asimismo, el sistema ha demostrado falencias en aspectos puntuales que no afectaron a la decisión final. Por lo tanto, el control humano resulta imprescindible para trasladar su uso al ámbito de la práctica judicial.

Finalmente, respecto de su aplicabilidad a otros contextos jurídicos, el GPT demuestra suficiente consistencia para ser utilizado en cualquier régimen provincial o nacional argentino. Su exportación a otros países también es posible, en la medida que se trate de sistemas de derecho continental, previa reconfiguración de un GPT similar adaptado a la legislación sustancial y procesal pertinente. En sistemas de *common law*, en cambio, el uso de este GPT personalizado sería más limitado, demandaría integrar jurisprudencia, rediseñar su lógica y realizar nuevos estudios e investigaciones para comprobar su adecuado funcionamiento.

Referencias

H. Álvarez Saez (2023), *Breve historia entre saberes jurídicos y no jurídicos, y de cómo facilitar la mitigación de las barreras gnoseológicas en tiempos de IA*, en J. Corvalán, "Tratado de Inteligencia Artificial y Derecho", tomo III, La Ley, 2023

B. Areán (2004), *Juicio de usucapión,* Hammurabi, 2004

J. Bueres (2014), *Código Civil y Comercial de la Nación analizado, comparado y concordado*, tomo II, Hammurabi, 2014

F. Causse, C. Pettis (2015), *Comentario al art. 1909,* en M. Herrera, G. Caramelo, S. Picasso, "Código Civil y Comercial de la Nación Comentado", tomo v, Infojus, 2015

F. Contini (2024), *Unboxing Generative AI for the Legal Professions: Functions, Impacts and Governance*, in "International Journal for Court Administration", vol. 15, 2024, n. 2

J.G. Corvalán, M. Carro (2023), *Más allá del juego de la imitación: las principales limitaciones de la inteligencia artificial*, en J.G. Corvalán (por), "Tratado de Inteligencia Artificial y Derecho", La Ley, tomo i, 2023

J.G. Corvalán, M. Sánchez Caparrós (2023), *Guía de directrices para el uso de ChatGPT e IA generativa de texto en la Justicia*, La Ley, 2023

E.J. Couture (1978), *Estudios de derecho procesal civil*, Ediciones Depalma, tomo ii, 1978

L.R. Flah, M. Smayevsky (1987), *La protección de los terceros y el proceso de usucapión*, in "La Ley", 1987, n. 29

F. García-Peñalvo, A. Vázquez-Ingelmo (2023), *What Do We Mean by GenAI? A Systematic Mapping of The Evolution, Trends, and Techniques Involved in Generative AI*, in "UNIR", 2023

M. García Sánchez (2023), *El abordaje de ChatGPT: el "Rinoceronte Gris" de la IA conversacional*, in "IUS ET SCIENTIA", vol. 9, 2023, n. 1

M. Ma, A. Sinha, A. Tandon, J. Richards (2024), *Generative AI Legal Landscape 2024*, CodeX, Stanford Law School, 2024

M.C. Martínez Nicholls, S.S. Marroquín (2024), *La inteligencia artificial y su incidencia en la valoración de la prueba en el proceso jurisdiccional*, Escuela de Derecho, Universidad EAFIT, Medellín, Tesis, 2024

G.A. Pardo (2024), *Cómo crear GPT educativo personalizado (ChatGPT Plus)*, 17 junio 2024

G.H. Quadri (2011), *La prueba en el proceso civil y comercial: teoría general, tipos de prueba, la prueba en los procesos en particular*, Abeledo-Perrot, 2011

M. Smayevsky (2007), *Usucapión,* La Ley, 2007

A. Vilchis Robles (2024), *Prolegómenos de inteligencia artificial en la impartición de justicia. Implicaciones prácticas y nuevos desafíos para los derechos humanos*, en "Revista Internacional y Comparada de Derechos Humanos", vol. 7, 2024, n. 1

J. Wei, Y. Tay, R. Bommasani et al. (2022), *Emergent Abilities of Large Language Models*, 2022

J. Wei, X. Wang, D. Schuurmans et al. (2022), *Chain-of-thought prompting elicits reasoning in large language models. Google Research, Brain Team*, 2022

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0212 • articolo sottoposto a peer review • pubblicato in anteprima il 20 mar. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Massimiliano Marletta

Blockchain e buona fede: riuscirà la tecnologia a sostituire la fiducia?

Il contributo esamina in profondità la complessa relazione tra *smart contracts* e principio di buona fede, che rappresenta un cardine fondamentale del diritto contrattuale tradizionale. Gli *smart contracts*, con le loro caratteristiche distintive di automazione, immutabilità e decentralizzazione, offrono significativi vantaggi in termini di efficienza e rapidità nell'esecuzione delle obbligazioni contrattuali. Tuttavia, queste innovazioni tecnologiche sollevano questioni critiche riguardanti la loro capacità di adeguarsi a circostanze impreviste e di rispettare gli obblighi di cooperazione e lealtà tra le parti coinvolte. Il contributo analizza se e come il principio di buona fede, che è consolidato nel diritto civile italiano e riconosciuto anche nei Princìpi Unidroit, possa essere applicato in modo efficace ai contratti digitali. A tal fine, vengono proposte soluzioni innovative, come l'inserimento di clausole di *hardship* automatizzate, che potrebbero garantire una maggiore flessibilità e protezione per le parti. Inoltre, viene approfondito il ruolo cruciale della trasparenza e degli obblighi informativi all'interno del contesto degli *smart contracts*, evidenziando le sfide che questi strumenti pongono alla fiducia reciproca tra le parti. L'obiettivo finale di questo lavoro è fornire un quadro critico e costruttivo per l'evoluzione della contrattualistica digitale, promuovendo un dialogo tra innovazione tecnologica e principi giuridici tradizionali.

Smart contracts – Buona fede – Equilibrio contrattuale – Automazione – Trasparenza

Blockchain and good faith principle: will technology be able to replace trust?

This paper examines in depth the complex relationship between smart contracts and the principle of good faith, which represents a fundamental cornerstone of traditional contract law. Smart contracts, with their distinctive characteristics of automation, immutability, and decentralization, offer significant advantages in terms of efficiency and speed in the execution of contractual obligations. However, these technological innovations raise critical questions regarding their ability to adapt to unforeseen circumstances and to uphold the obligations of cooperation and loyalty among the parties involved. The paper analyzes whether and how the principle of good faith, which is established in Italian civil law and also recognized in the Unidroit Principles, can be effectively applied to digital contracts. To this end, innovative solutions are proposed, such as the inclusion of automated hardship clauses, which could ensure greater flexibility and protection for the parties. Furthermore, the crucial role of transparency and informational obligations within the context of smart contracts is explored, highlighting the challenges these tools pose to mutual trust among the parties. The ultimate goal of this work is to provide a critical and constructive framework for the evolution of digital contracting, promoting a dialogue between technological innovation and traditional legal principles.

Smart contracts – Good faith – Contractual equilibrium – Automation – Transparency

L'Autore è dottorando in Analisi economica del diritto presso l'Università di Catania, Dipartimento di Economia e commercio e visiting PhD scholar presso l'Istituto di Diritto ed economia di Amburgo

Sommario: 1. Introduzione. – 2. *Smart contracts*: profili strutturali e funzionali. – 3. La portata del canone di buona fede nel diritto tradizionale. – 4. La buona fede nell'ambito degli *smart contracts*: possibili conflitti e soluzioni. – 5. La Regolazione Europea: implicazioni delle lacune sulla buona fede nei contratti *smart*. - 6. Riflessioni conclusive: verso una nuova era della contrattualistica.

1. Introduzione

Ogni contributo scientifico che miri a indagare l'impatto della rivoluzione digitale sul panorama giuridico finisce con l'affrontare, ad un certo punto della trattazione, una questione fondamentale scandita dal seguente interrogativo: "Bisognerebbe allineare il diritto all'innovazione tecnologica o, viceversa, l'impiego di quest'ultima dovrebbe essere allineato al diritto vigente?".

Tale interrogativo fa da sfondo anche al tema che ci si propone di esaminare, ossia quello riferibile ai rapporti tra *smart contracts* e principio di buona fede.

Assunta l'esistenza di questa dicotomia tra il diritto vigente ed i profili di innovazione tecnologica, essa si rivela appunto cruciale nell'ambito degli *smart contracts*, consistenti in contratti auto-esecutivi che operano su sistemi di *blockchain*[1].

Se, per un verso, essi tendono a soddisfare irrinunciabili istanze di efficienza e trasparenza[2], dall'altro, sollevano un ampio ordine di problemi di complessa risoluzione. A questo proposito, giova rammentare che la letteratura di riferimento si è perlopiù soffermata circa gli effetti da essi riverberati sulla "anatomia fondamentale" dell'istituto contrattuale, ossia sugli elementi essenziali di cui all'articolo 1325 del codice civile[3].

I caratteri di rigidità ed immutabilità insiti nei meccanismi di programmazione di detto sistema automatizzato pongono sfide uniche anche con riferimento all'applicazione del principio di buona fede, il quale impone un contegno leale e corretto tra le parti[4].

Nella tradizione giuridica di diritto continentale, il principio di buona fede gioca un ruolo di primo ordine nel garantire che i contraenti si comportino, conformemente al canone solidaristico di cui all'articolo 2 della Costituzione, in modo equo e responsabile lungo tutto l'arco della vicenda contrattuale, partendo dalla fase delle trattative sino a giungere alla conclusione del programma negoziale[5]. Tuttavia, la natura automatica degli *smart contracts* postula che tali princìpi

1. La *blockchain* consiste in un registro digitale atto a salvare dati in modo sicuro. Ciò avviene in forza del fatto che i dati sono organizzati in blocchi tra loro collegati e dunque non sono suscettibili di modifica.
2. Brandstätter–Schulte–Cito–Borkowski 2020.
3. In particolare, la letteratura giuridica di riferimento sul tema ha affrontato svariate volte la questione inerente alla forma e all'accordo, enfatizzando come questi concetti presentino delle declinazioni peculiari nel contesto dei contratti digitali insuscettibili di essere compresi a pieno se analizzati con la lente del diritto tradizionale.
4. Hewa–Ylianttila–Liyanage 2021.
5. L'elaborazione dottrinale in materia di buona fede rappresenta la manifestazione più tangibile dell'applicazione del principio solidaristico nell'ambito del diritto privato. Ciò in base all'assunto per il quale il buon funzionamento dei mercati non può che essere implementato attraverso una dimensione altruistica che connoti le relazioni tra le parti.

debbano essere ripensati e reinterpretati[6]. Si tratta di rinvenire – se possibile – l'esistenza di una soluzione che permetta di coniugare due universi ontologicamente opposti: da un lato, quello della "culpa in contrahendo", congegnato dal legislatore in relazione a un ideale scenario di rilevante, per non dire pervasiva, relazione umana; dall'altro, quello dei contratti automatizzati, privi di un sostrato relazionale, che lasciano uno spazio assai ridotto, se non del tutto nullo, alla discrezionalità ed all'interpretazione.

Tramite una riflessione critica ed un approfondimento delle implicazioni normative e pratiche, si mira a delineare un quadro che consenta di rispondere a interrogativi cruciali concernenti il futuro della contrattualistica nell'era digitale.

2. *Smart contracts*: profili strutturali e funzionali

Gli *smart contracts* costituiscono un'innovazione significativa e dall'impatto progressivamente crescente nel campo del diritto e dell'economia. La letteratura tradizionale è concorde nel definirli quali programmi informatici che eseguono automaticamente le clausole di un contratto, basandosi su condizioni predefinite[7].

I tratti strutturali che li connotano sono dati dall'automazione, dall'immutabilità e dalla decentralizzazione.

Quanto al primo profilo, esso si giustifica in relazione al fatto che essi eseguono immediatamente le clausole contrattuali al verificarsi di determinati eventi senza la necessità di ricorrere a intermediari e riducendo, pertanto, i costi di transazione[8]. Si tratta di un requisito che ha fortemente esaltato la vocazione efficientistica di detto istituto, consentendo una più agile allocazione delle risorse. Atteso che, fisiologicamente, il contratto dovrebbe fungere da strumento atto a spostare le risorse verso usi maggiormente valutati (e dunque da un soggetto che valuti meno una determinata risorsa ad uno che la valuti di più), la prospettiva di un procedimento più snello dovrebbe assurgere a stimolante incentivo per la conclusione di accordi che altrimenti avrebbero luogo più difficilmente o che non avrebbero luogo completamente[9].

Il tratto dell'immutabilità lo si spiega in ragione dell'immodificabilità del contratto: a partire dal momento in cui esso è stato implementato sulla *blockchain*, non può subire modifiche senza il consenso della totalità delle parti. Si tratta di uno dei caratteri maggiormente problematici, atteso che dalla rigidità del contratto potrebbero derivare dei conflitti tra i contraenti in punto di gestione delle sopravvenienze[10].

Il terzo profilo strutturale (la decentralizzazione), dal tenore più strettamente ingegneristico, attiene alla "distribuzione del controllo". Esso è un principio operativo mediante il quale il controllo, la gestione e la governance del sistema sono distribuiti su più nodi, anziché in un singolo ente o autorità centrale[11]. In termini più semplici, il potere e la responsabilità del sistema vengono distribuiti tra tutti i partecipanti. La finalità associatavi è quella di garantire la resistenza e la piena trasparenza del sistema: poiché i dati e le operazioni non vengono centralizzate in un singolo punto, un malfunzionamento in un nodo non compromette l'intera rete. Tuttavia – rovescio della medaglia – vi è da segnalare che l'assenza di un'autorità centrale complica la risoluzione di eventuali controversie, i cui meccanismi compositivi vengono demandati alle

6. De Filippi–Wright 2018.
7. Szabo 1997.
8. Quello dei costi di transazione è problema comune alla scienza giuridica ed economica. Tuttavia, il diverso approccio seguito ha portato talvolta a conclusioni opposte: da un lato, gli economisti, più attenti ai profili di efficienza economica, hanno guardato con maggior favore all'impiego di detti strumenti; dall'altro, i giuristi hanno palesato una certa diffidenza in relazione alle implicazioni giuridiche sottese.
9. Wang–Yuan–Wang et al. 2018.
10. Peraltro, questo carattere di inflessibilità in punto di gestione delle sopravvenienze finirebbe col rendere meramente apparente la duttilità di tale strumento.
11. Werbach 2018.

parti per il tramite di meccanismi da integrare nel contratto stesso[12].

Dalla disamina di tali tratti emerge *ictu oculi* l'esistenza di profonde differenze rispetto ai contratti tradizionali. Esse investono, per così dire, aspetti di macroscopica rilevanza nella dinamica della vicenda e dell'istituto contrattuale, dalla struttura, alle modalità di adempimento, alle modalità di risoluzione dei conflitti[13]. In particolare, malgrado la fisionomia degli *smart contracts* assicuri efficienza e rapidità nelle transazioni, essa contribuisce a creare un "ambiente" nel quale il principio della buona fede potrebbe non essere osservato a pieno.

In concreto, la programmazione rigida rappresenta un significativo ostacolo per le parti laddove vi sia l'esigenza di gestire le sopravvenienze, potendosi conseguentemente profilare una situazione patologica ove le parti rimangano vincolate ad un negozio che non riflette più le loro intenzioni originali[14].

Dinnanzi a tali scenari, diviene essenziale interrogarsi su come (e se) la buona fede possa essere mantenuta. L'intrinseca inflessibilità di tali strumenti, teoricamente, secondo taluni, dovrebbe essere colmata da una oculata previsione delle parti circa le contingenze che potrebbero verificarsi lungo la relazione contrattuale, inoculando all'interno dell'accordo medesimo un "ordinamento sezionale", alla stregua del modello del contratto-normativo[15], peraltro non ignoto al nostro sistema giuridico.

Tuttavia, la questione non risulta essere di così semplice risoluzione. A questo proposito, rimane di estrema attualità l'insegnamento fornitoci da Piero Calamandrei: "Per quanto cerchi di essere completo e coprire tutti gli spazi vuoti, l'ordinamento giuridico è paragonabile alla mano che tenti di toccare il polso. Per quanto vi si avvicini, non ci riuscirà mai"[16].

3. La portata del canone di buona fede nel diritto tradizionale

Come noto, il principio di buona fede è comune a vari rami del diritto. Ciò si spiega in relazione all'assunto per cui esso funge da modello comportamentale a cui ogni relazione giuridica deve conformarsi: non solo, dunque, le parti che negoziano in sede di trattativa, ma anche l'amministrazione ed il cittadino durante l'espletarsi del procedimento amministrativo[17] ed i soggetti portatori di interessi opposti nel processo.

Ferma questa consapevolezza, in questa sede si intende porre la lente nell'ambito del diritto civile, ove tale principio ha trovato una significativa elaborazione dottrinale e giurisprudenziale.

A livello normativo, il principio di buona fede è formalmente riconosciuto nell'articolo 1375 del codice civile, ai cui sensi è previsto che "Il contratto deve essere eseguito secondo buona fede".

Si tratta, come può agevolmente constatarsi, di una clausola generale[18], la cui determinazione in punto di significato ha abbisognato di una forte opera di implementazione giudiziale.

Come fatto notare da accurata dottrina, tale principio ha subito nel corso dei decenni delle profonde rivisitazioni, legate alla necessità di rapportarne la portata alla crescente complessità delle transazioni economiche, in guisa da soddisfare

12. Secondo taluni, le difficoltà nella gestione delle controversie potrebbe condurre a un comportamento collaborativo tra le parti nell'ottica del comune interesse a non dare luogo all'insorgenza di liti. Esso opererebbe alla stregua di un deterrente che finirebbe col favorire una cooperazione ancora più marcata tra le parti contraenti, specialmente nei casi in cui il contratto digitale difetti di una clausola compromissoria.
13. Cerrato 2019.
14. Savelyev 2017.
15. Il riferimento al modello del contratto normativo non è complesso da cogliere: atteso che gli *smart contracts* sono per natura rigidi ed automatizzati, si rende di conseguenza necessaria la profilazione di un "quadro normativo" che regoli fasi future ed eventuali nell'esecuzione del programma negoziale.
16. Calamandrei 2008.
17. L'applicabilità del canone di buona fede nell'ambito del diritto amministrativo si spiega in ragione del fatto che attraverso l'instaurazione del procedimento viene a configurarsi tra amministrazione e cittadino un "contatto sociale qualificato".
18. Nicolussi–Portonera 2023.

il canone costituzionale di solidarietà (il quale, da lungo tempo, ha conosciuto numerose applicazioni nel campo del diritto contrattuale). In particolare, la necessità di fronteggiare fallimenti del mercato quali asimmetrie informative[19] e posizioni di disparità sotto il profilo della forza contrattuale ha condotto ad un significativo ampliamento della sua area di significato. Volendo ripercorrere brevemente, ma in modo (auspicabilmente) efficace le tappe di un lunghissimo e assai complesso processo evolutivo, si darà contezza delle "tre stagioni" che hanno interessato il ciclo vitale di detto principio.

A partire dalla codificazione del 1942 e nei tre decenni appena successivi, la buona fede è stata concepita restrittivamente[20]: essa si limitava a rappresentare un principio guida per il comportamento delle parti, avente l'intento di favorire la cooperazione e la trasparenza nel corso delle trattative e nell'esecuzione delle obbligazioni. Tuttavia, a livello pratico, la violazione di obblighi precontrattuali non veniva sanzionata e quindi la di tutela era pressoché del tutto ineffettiva[21].

Ciò lo si poteva spiegare in ragione della complessità dei rapporti tra giuspositivismo, codificazione ed ascesa del liberismo, avendo ciò generato un restringimento dell'influenza della buona fede sui sistemi giuridici dell'epoca. In particolare, nel nostro ordinamento giuridico, l'affermarsi delle concezioni soggettivistiche nella teoria del negozio giuridico, fondate sul dogma della volontà, portò all'emersione di un orientamento volto a ridurre il ruolo della regola della buona fede.

Un approccio diverso rispetto alla portata della buona fede lo si è registrato a partire dal momento in cui ha cominciato ad avere luogo quel processo di rilettura del codice civile alla luce dei canoni costituzionali, in ragione dell'esaltazione dell'assunto solidaristico fissato dall'articolo 2 della Legge Fondamentale.

A partire dagli anni Ottanta e Novanta, si è assistito al consolidamento del concetto di buona fede integrativa.

Questo approccio ha messo in evidenza la necessità di un'interpretazione più dinamica della buona fede, sottolineando l'importanza della collaborazione tra le parti e il rispetto delle aspettative reciproche[22]. Si tratta di un mutamento radicale nell'interpretazione di siffatto principio, il quale, da clausola meramente valutativa, assurge a clausola immediatamente precettiva, con funzione integrativa del rapporto obbligatorio, fonte di obbligazioni strumentali all'adempimento, sia dal lato del debitore che da quello del creditore.

Durante questa fase, è emersa l'idea che la buona fede non dovesse limitarsi al momento della conclusione del contratto, ma dovesse permeare tutte le fasi della relazione contrattuale.

Gli operatori economici e i giuristi hanno iniziato a riconoscere che il principio di buona fede poteva e doveva essere utilizzato per risolvere le controversie legate all'esecuzione dei contratti, promuovendo un ambiente di fiducia e cooperazione[23].

Questo sviluppo ha portato a un'importante evoluzione della giurisprudenza, con decisioni che hanno sottolineato l'obbligo delle parti di comportarsi lealmente e di non adottare atteggiamenti opportunistici. I tribunali hanno iniziato a interpretare le clausole contrattuali in modo tale da riflettere non solo il testo del contratto, ma anche le intenzioni delle parti, cercando di preservare l'equilibrio e la giustizia nelle relazioni contrattuali.

Negli ultimi anni, a fronte dell'emersione di nuove tecnologie e modelli di business, il concetto di buona fede ha subito un'ulteriore trasformazione, dando vita a quella che possiamo definire buona fede creativa[24]. Questo nuovo approccio riflette la necessità di adattarsi a un contesto commerciale in rapido cambiamento, dove le circostanze

19. Tale estensione della portata del canone di buona fede è seguita alla crisi del paradigma pan-liberistico.
20. Scolaro–Zannini Quirini 2020.
21. Non a torto, la dottrina dell'epoca era concorde nel definire siffatta norma come un "precetto senza sanzione".
22. Marletta–Mastroianni 2024.
23. Alpa 2001.
24. La nota teoria del contatto sociale qualificato (parimenti nota come teoria degli "obblighi di protezione senza prestazione") trae la propria giustificazione dogmatica proprio dalla concezione creativa della buona fede.

possono mutare velocemente e le parti sono chiamate a rispondere in modo flessibile e innovativo[25].

La buona fede creativa non si limita a garantire il corretto adempimento delle obbligazioni dedotte in contratto o comunque afferenti alla vicenda contrattuale, ma crea nuove obbligazioni, invitando le parti a collaborare attivamente per modificare o integrare i contratti in base a eventi imprevisti o che compromettano significativamente i fondamentali risultati attesi dalle parti e sottesi alla stipula dell'accordo medesimo.

4. La buona fede nell'ambito degli *smart contracts*: possibili conflitti e soluzioni

Nel contesto degli *smart contracts*, la questione della buona fede si fa sfaccettata e complessa, in ragione delle peculiarità connaturate a detti strumenti automatizzati[26]. La buona fede, come principio cardine del diritto contrattuale, assume un significato che deve necessariamente essere reinterpretato o, se vogliamo, calato in uno scenario ove le interazioni umane sono mediate dalla tecnologia, e dove l'automazione può ridurre o eliminare la discrezionalità delle parti.

Come già fatto presente, la buona fede si è sviluppata in un contesto di relazioni umane ove sia l'applicazione che l'interpretazione del contratto erano del tutto influenzate dalla comunicazione nonché dalla cooperazione tra le parti. Giova ricordare che siffatto profilo è stato esaltato dalla concezione integrativa, prima, e creativa poi, dello stesso principio: entrambe le concezioni, infatti, evidenziano l'indispensabilità di un costante contegno comunicativo e cooperativo tra le parti, sia in condizioni di fisiologia che in situazioni di crisi e incertezza della vicenda contrattuale. Tuttavia, con l'avvento degli *smart contracts*, questo modello è stato messo alla prova.

La questione centrale attiene all'adattamento del canone di buona fede alle peculiarità degli *smart contracts*, i quali, sebbene possano offrire degli indubbi vantaggi in punto di efficienza, introducono anche rigidità nel loro funzionamento.

Uno degli aspetti critici è la capacità di questi contratti di affrontare le variazioni delle circostanze che potrebbero influenzare il loro adempimento. In particolare, eventi imprevisti possono causare un'alterazione dell'equilibrio contrattuale.

Invero, il problema delle sopravvenienze ha investito anche il diritto comune, attesa l'insufficienza del rimedio della risoluzione per eccessiva onerosità, la cui applicazione resta confinata ad una casistica abbastanza eccezionale[27].

Facendo leva sul canone di buona fede, il quale impone alle parti, entro i limiti di un sacrificio non eccessivamente dispendioso, di considerare anche gli interessi altrui, la giurisprudenza italiana ha giudicato con favore, in quanto atte a proteggere interessi meritevoli di tutela, le clausole di *hardship*[28].

Dette clausole non sono espressamente previste nel codice civile italiano e trovano il loro referente normativo nella Convezione di Vienna del 1980 sulla vendita internazionale dei beni[29].

Tuttavia, il loro impiego, invalso in via di prassi, ha conosciuto una progressiva diffusione in ragione della duttilità dell'istituto. Trattasi di disposizioni contrattuali che consentono la rinegoziazione dei termini di un contratto quando eventi imprevedibili e non imputabili alle parti alterano significativamente l'equilibrio economico originario, rendendo l'adempimento eccessivamente oneroso per una di esse[30]. Pur non comportando l'impossibilità della prestazione, siffatte clausole sono

25. Natalini 2011.
26. Raskin 2017.
27. Il regime normativo della risoluzione per eccessiva onerosità sopravvenuta può infatti invocarsi esclusivamente a fronte di eventi straordinari e imprevedibili.
28. Bianca 2011.
29. Essa ha un ambito di copertura soggettivo e oggettivo limitato, in quanto si applica esclusivamente alle vendite internazionali di beni tra le parti che hanno sede in Stati aderenti alla Convezione medesima. Tali disposizioni di diritto internazionale particolare non si applicano, tuttavia, a vendite di beni per uso personale, beni immobili, titoli o servizi.
30. Tuttavia, a differenza di quanto previsto in ordine alla risoluzione per eccessiva onerosità, non è necessario che l'evento sia connotato dal crisma della straordinarietà.

finalizzate alla conservazione della continuità contrattuale tramite un adattamento delle condizioni, promuovendo la cooperazione tra le parti e prevenendo la risoluzione immediata del contratto[31].

Spostando l'attenzione agli *smart contracts*, ci si chiede se l'uso di queste clausole possa rappresentare una soluzione idonea a preservare l'equilibrio contrattuale nel caso di sopravvenienze e rendere effettivo il principio della buona fede e di cooperazione tra le parti[32].

La rigidità scaturente dalla loro esecuzione automatica e vincolata al codice programmato potrebbe infatti essere attenuata attraverso l'inserimento di meccanismi contrattuali che consentano l'attivazione di clausole di *hardship* in determinate condizioni. L'estensibilità di queste clausole potrebbe essere implementata tramite sistemi di *trigger* automatici: se un certo evento o cambiamento di circostanze, previamente definito, si verifica, lo *smart contract* potrebbe attivare un protocollo di rinegoziazione o sospendere temporaneamente l'esecuzione delle obbligazioni[33].

Per esempio, uno *smart contract* potrebbe essere programmato per monitorare determinati indicatori economici o giuridici, come le variazioni significative nei tassi di cambio o nel livello dei prezzi[34]. Se il valore di tali indicatori superasse una soglia prestabilita, il contratto attiverebbe automaticamente la clausola di *hardship*, sospendendo le obbligazioni dedotte fintantoché le parti non abbiano raggiunto un nuovo accordo. Questo tipo di estensibilità permette agli *smart contracts* di adattarsi a scenari imprevisti senza compromettere l'equità delle relazioni contrattuali.

Tuttavia, per quanto un qualche ottimismo al riguardo possa senza dubbio dirsi fondato, tale problema non sarebbe di così agevole risoluzione. Ciò in quanto l'applicazione delle clausole di *hardship* negli *smart contracts* non si esaurisce in una mera operazione di programmazione tecnica. Esistono anche questioni giuridiche delicate, come la definizione esatta di ciò che costituisce una circostanza di *hardship* e come tale circostanza debba essere gestita a livello pratico. È fondamentale che le parti contrattuali anticipino non solo gli eventi che potrebbero attivare la clausola, ma anche le modalità con cui il contratto si adatterà a tali eventi. Questo potrebbe includere, per esempio, una procedura automatizzata di risoluzione delle controversie o l'impiego di terze parti fidate per determinare se le condizioni di *hardship* siano effettivamente soddisfatte.

In ogni caso, laddove la valutazione circa la bontà dell'estensione di tali clausole si esaurisca positivamente, diverrebbe indispensabile congegnare *smart contracts* assai più sofisticati, i quali vadano ben oltre la semplice automazione delle prestazioni.

Sebbene, sotto il profilo pratico, la questione dei rapporti tra contratti digitali ed articolo 1375 del codice civile investa specialmente il problema delle sopravvenienze, altri ordini di problemi si pongono sul piano della trasparenza e degli obblighi informativi[35].

Quanto alla trasparenza, essa rappresenta un concetto primariamente rilevante in un contesto nel quale non di rado la fiducia tra le parti è spesso messa alla prova da dinamiche economiche complesse ed asimmetrie informative[36].

Per un verso, gli *smart contracts*, attraverso il loro funzionamento basato su *blockchain*, assicurano una maggiore chiarezza operativa, permettendo a tutte le parti di avere accesso alle medesime informazioni riguardanti il contratto.

Dall'altro, questa declinazione della trasparenza potrebbe rivelarsi ambivalente se non

31. Si tratterebbe di una significativa applicazione, nel solco della continuità rispetto al diritto comune, del principio della conservazione del contratto.

32. Teubner 2000.

33. Venturelli 2017.

34. Bartoletti–Pompianu 2017.

35. Il complesso rapporto tra trasparenza e strumenti digitali o di intelligenza artificiale è un tema che ha interessato non solo il diritto privato, ma anche il ramo amministrativo. In letteratura, il dibattito sul punto è stato alimentato in relazione all'impiego di procedure algoritmiche nell'ambito del procedimento.

36. Piatti 2016.

accompagnata da un'adeguata comprensibilità, finendo dunque paradossalmente con il rinnegare sé stessa[37].

La *blockchain*, pur essendo un mezzo potentemente democratizzante nel senso sopra specificato, presenta una barriera linguistica e culturale significativa. I contratti *smart* sono scritti in linguaggi di programmazione specifici, come *Solidity*, il che può risultare inaccessibile a coloro che non possiedono competenze tecniche adeguate. Ciò implica che, malgrado l'informazione sia tecnicamente accessibile, il suo significato possa rimanere oscuro per gran parte degli utenti e di converso totalmente non intellegibile.

Inoltre, laddove una delle parti avesse una maggiore familiarità con il codice, essa potrebbe sfruttare questa situazione a proprio vantaggio, creando un contesto di potenziale speculazione o manipolazione. Riecheggia a gran voce un insegnamento tradizionale e più volte ribadito dalla giurisprudenza di legittimità: la trasparenza non è solo una questione di visibilità delle informazioni, ma anche di comprensione, intellegibilità e interpretazione. La necessità di garantire una trasparenza effettiva sottende l'esigenza di standardizzare e semplificare il linguaggio utilizzato nei contratti, affinché tutte le parti possano comprenderne il contenuto senza necessitare di esperti esterni. Solo così si possono evitare malintesi che possono compromettere la buona fede tra le parti.

In aggiunta, la questione della trasparenza si intreccia con le vulnerabilità intrinseche della tecnologia *blockchain*. Sebbene la decentralizzazione rappresenti un vantaggio in termini di sicurezza, non esiste una garanzia assoluta avverso le frodi informatiche o i malfunzionamenti del sistema. La scoperta di bug nel codice o attacchi informatici rappresentano rischi concreti che possono compromettere l'affidabilità di un contratto. Inoltre, l'immutabilità, che è uno dei punti di forza degli *smart contracts*, diventa un'arma a doppio taglio: se il codice originale contiene errori o ambiguità, una volta attuato il contratto, le parti sono vincolate a condizioni che potrebbero non riflettere le loro intenzioni originarie.

Ciò porta a considerare la necessità di meccanismi di revisione e auditing del codice, per garantire che ogni clausola sia chiara, comprensibile e coerente con le aspettative delle parti[38]. In sintesi, la trasparenza nei meccanismi degli *smart contracts* non deve essere intesa come un mero accesso alle informazioni, ma come un processo che richiede chiarezza e comprensione reciproca. Solo così si può garantire una reale osservanza del principio di buona fede.

Spostando infine la focale sugli obblighi informativi, ci si interroga in particolare sull'effettiva portata di siffatto obbligo in un contesto contrassegnato dalla difficoltà di comunicazione tra le parti e da enorme complessità tecnica[39].

Nel contesto dei contratti automatizzati, la difficoltà principale risiede nel fatto che l'obbligo di informazione non si limita alla mera comunicazione di dati, ma deve estendersi alla comprensione del funzionamento del contratto stesso. Se una delle parti non ha accesso a informazioni chiave o, peggio, non è in grado di comprendere il funzionamento del codice che regola il contratto, il rischio di entrare in una relazione contrattuale squilibrata aumenta notevolmente. La parte meno informata potrebbe trovarsi a fronteggiare rischi che non aveva previsto, potendo comportare la violazione del principio di buona fede. È imperativo, pertanto, che tutte le parti siano educate e informate riguardo alle tecnologie utilizzate, nonché ai diritti e agli obblighi che ne derivano.

Inoltre, la questione si complica ulteriormente quando si considerano le clausole di esclusione della responsabilità o le limitazioni di adempimento. Queste clausole, se non comunicate e comprese adeguatamente, possono avere un impatto devastante sui diritti delle parti coinvolte.

La loro introduzione in un contratto *smart* potrebbe avvenire in modo così sottile da sfuggire all'attenzione di una delle parti, minando la fiducia e la buona fede necessarie per una relazione contrattuale sana. Pertanto, la responsabilità di garantire che tutte le informazioni siano chiaramente comunicate e comprese ricade non solo sulla parte più esperta, ma deve essere un impegno condiviso.

37. Janssen–Patti 2020.

38. Gaeta–Aulino–Troisi 2023.

39. Tosi 2010.

Infine, è essenziale che gli operatori del settore, i giuristi e i programmatori lavorino insieme per sviluppare soluzioni che possano migliorare l'obbligo di informazione e promuovere un approccio collaborativo[40]. Ciò potrebbe includere la creazione di guide pratiche, l'utilizzo di linguaggi più accessibili per il codice e l'implementazione di meccanismi di feedback che consentano alle parti di chiarire i propri dubbi prima della finalizzazione del contratto.

In questa ottica, la cooperazione tra esperti di diritto e tecnici diventa cruciale per garantire che l'obbligo di informazione non si risolva in una mera dimensione formale[41], ma che assurga ad elemento essenziale per la realizzazione di contratti giusti ed equi. La mancata osservanza di tale obbligo potrebbe, infatti, condurre a conseguenze legali significative, come la nullità del negozio o il risarcimento dei danni, conducendo ad uno scenario di patologia della vicenda contrattuale.

5. La regolazione europea: implicazioni delle lacune sulla buona fede nei contratti *Smart*

Volgendo lo sguardo al diritto dell'Unione europea, può rammentarsi di come la questione inerente ai rapporti tra contratti digitali e buona fede non sia stata adeguatamente affrontata a livello normativo[42].

Malgrado il legislatore comunitario abbia perpetuamente promosso l'innovazione digitale, non ha al contempo fornito una compiuta disciplina in merito agli *smart contracts* nel contesto dei princìpi del diritto civile tradizionale, come la buona fede[43].

Tale lacuna normativa genera tensioni significative, specie alla luce della necessità di garantire obiettivi di primo ordine quali l'equilibrio contrattuale e la cooperazione tra le parti contraenti.

A livello di regolamentazione vigente, le fonti di riferimento sono rappresentate dal *Digital Markets Act* e dal *Digital Services Act*[44], i quali si limitano a stabilire norme generalissime e di portata meramente programmatica in ordine alla trasparenza dei servizi digitali, senza affrontare direttamente le problematiche legate alla governance ed all'esecuzione dei contratti automatizzati.

Inoltre, può farsi richiamo della Direttiva 2019/770, la quale disciplina i contratti di fornitura di contenuti digitali[45]. Tuttavia, essa non si presta ad essere un adeguato riferimento in tema di *smart contracts* poiché non tiene debitamente conto delle specificità degli stessi rispetto al tipo contrattuale che mira a regolamentare, lasciando totalmente indefinito il problema relativo all'osservanza del canone di buona fede.

In particolare, siffatta direttiva pone la lente esclusivamente sui contratti di fornitura dei servizi digitali, i quali presentano una struttura assai più basica rispetto agli *smart contracts*. Di conseguenza difettano strumenti idonei ad affrontare i problemi sottesi alla rigidità, all'informazione asimmetrica e alla rinegoziazione automatizzata. Inoltre, la direttiva è silente in merito all'individuazione di meccanismi di *enforcement*, non prevedendosi né un'autorità centrale, né un meccanismo di risoluzione interno al sistema.

Ciò rende particolarmente complessa la gestione delle transazioni transfrontaliere, ove la diversità normative tra Stati membri può portare ad interpretazioni diverse su questioni cruciali[46].

Alla luce del quadro delineato, emerge che, così come strutturata attualmente, la regolamentazione europea non è in grado di garantire un'efficace

40. Ciò esalta la dimensione necessariamente multidisciplinare di tale tematica tanto sotto il profilo teorico quanto sul versante pratico.
41. Vestoso 2021.
42. La normativa europea è strutturata sotto il profilo dei contenuti non dissimilmente da quella interna: essa riconosce all'interno dei Princìpi Unidroit la buona fede, ma non prevede un apparato disciplinare che consenta di declinare detto canone nell'ambito dei contratti digitali.
43. Addante 2017.
44. Ibáñez Colomo 2021.
45. Capilli 2023.
46. Tosi 2021.

applicazione del principio di buona fede nel contesto degli *smart contracts*.

Allo scopo di colmare dette lacune, si presenta come indispensabile e fortemente auspicato un intervento normativo che armonizzi l'impiego degli *smart contracts* con i princìpi del diritto contrattuale europeo, prevedendo meccanismi di rinegoziazione automatica e di *enforcement* specifici al fine di garantire una sostanziale tutela delle parti coinvolte.

In mancanza di un'adeguata regolamentazione, si prospetta il rischio che siffatti strumenti riducano la protezione giuridica dei contraenti, trasformandosi così in mezzi distorsivi generatori di inefficienze[47].

6. Riflessioni conclusive: verso una nuova era della contrattualistica

In conclusione, l'analisi della relazione tra gli *smart contracts* e il principio di buona fede rivela non solo la necessità di un'interpretazione giuridica innovativa, ma anche un ripensamento profondo delle modalità contrattuali tradizionali. L'emergere delle tecnologie *blockchain* e degli *smart contracts* ha sfidato le nozioni consolidate di obbligazioni contrattuali, richiedendo un aggiornamento delle normative esistenti e l'inclusione di strumenti giuridici capaci di rispondere alle esigenze di flessibilità, adattamento e resilienza in contesti economici sempre più complessi e dinamici[48].

L'inserimento di clausole di *hardship* negli *smart contracts* si colloca al centro di questa evoluzione. Tali clausole non possono essere considerate semplici appendici contrattuali, ma piuttosto strumenti essenziali per garantire che le parti contrattuali possano affrontare in modo equo le incertezze e le contingenze del mercato. La capacità di adattarsi a situazioni impreviste è cruciale per preservare la buona fede, elemento fondamentale per il mantenimento di relazioni contrattuali armoniose e durature. Essa deve essere interpretata non solo come un dovere di lealtà e correttezza, ma anche come un principio dinamico che si evolve con le circostanze, permettendo alle parti di trovare soluzioni che rispettino gli equilibri economici inizialmente pattuiti.

Tuttavia, l'implementazione di tali clausole all'interno degli *smart contracts* presenta sfide significative. È fondamentale sviluppare un framework normativo chiaro e articolato, in grado di affrontare le questioni di responsabilità e di interpretazione giuridica che sorgono in questo nuovo contesto. La trasparenza nei processi decisionali e la chiara definizione di ruoli e responsabilità in caso di malfunzionamento degli *smart contracts* diventeranno aspetti cruciali per la fiducia degli utenti e l'adozione di queste tecnologie nel mondo degli affari[49]. Un quadro normativo ben definito non solo favorirà la stabilità delle relazioni commerciali, ma garantirà anche che le parti possano contare su un meccanismo di risoluzione delle controversie efficace e giusto.

Inoltre, la continua evoluzione delle tecnologie *blockchain* e degli *smart contracts* richiede un dialogo attivo e costruttivo tra giuristi, tecnologi e parti coinvolte. Solo attraverso una collaborazione fruttuosa e un approccio multidisciplinare sarà possibile sviluppare soluzioni che siano sia tecnicamente solide sia giuridicamente valide.

Questo non solo promuoverà l'innovazione, ma garantirà anche che i diritti e gli interessi delle parti siano rispettati e protetti. L'integrazione di esperienze e competenze diverse potrà dare vita a strumenti giuridici che riflettano le reali esigenze del mercato, incrementando la fiducia nel sistema contrattuale digitale.

Infine, il futuro della contrattualistica digitale è promettente, ma richiede una riflessione costante e un adattamento delle normative esistenti. L'equilibrio tra innovazione e protezione dei diritti fondamentali dovrà essere mantenuto affinché gli *smart contracts* possano realmente contribuire a un sistema economico più efficiente e giusto.

In questa prospettiva, la buona fede non deve essere vista come un principio statico, ma come un valore dinamico che evolve in simbiosi con le nuove forme di contratto, garantendo che la giustizia e l'equilibrio rimangano al centro delle relazioni commerciali nel XXI secolo.

Pertanto, è cruciale che le istituzioni, le organizzazioni e i professionisti del diritto si impegnino a

47. Ciò dimostra che il binomio digitalizzazione-efficienza ha senso solamente laddove le tecnologie siano accuratamente congegnate.

48. Giancaspro 2017.

49. Taherdoost 2023.

costruire un ecosistema giuridico che abbracci le potenzialità offerte dagli *smart contracts*, promuovendo al contempo una cultura della legalità e della responsabilità[50]. Solo in questo modo si potrà garantire un utilizzo equo e sostenibile di queste tecnologie, assicurando che i benefici siano distribuiti in modo equo tra tutte le parti coinvolte e contribuendo così a una crescita economica inclusiva e sostenibile.

Riferimenti bibliografici

A. Addante (a cura di) (2017), *Tutela del consumatore nei contratti telematici e nuove frontiere del diritto europeo della vendita*, Cedam, 2017

G. Alpa (2001), *Appunti sulla buona fede integrativa nella prospettiva storica e del commercio internazionale*, in "I contratti", 2001, n. 7

M. Bartoletti, L. Pompianu (2017), *An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns*, in M. Brenner, K. Rohloff, J. Bonneau et al. (eds.), "Financial Cryptography and Data Security - FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Revised Selected Papers 21", Springer, 2017

M.R. Bianca (2011), *Alcune riflessioni sul concetto di meritevolezza degli interessi*, in "Rivista di diritto civile", vol. 57, 2011, n. 6

T. Brandstätter, S. Schulte, J. Cito, M. Borkowski (2020), *Characterizing Efficiency Optimizations in Solidity Smart Contracts*, in "2020 IEEE International Conference on Blockchain (Blockchain)", IEEE, 2020

P. Calamandrei (2008), *Fede nel diritto*, a cura di Silvia Calamandrei, Laterza, 2008

G. Capilli (2023), *Le modifiche e l'aggiornamento del contenuto digitale e dei servizi digitali nella disciplina di attuazione delle direttive (UE) 770 e 771 del 2019*, in "MediaLaws", 2023, n. 1

S.A. Cerrato (2019), *Contratti tradizionali, diritto dei contratti e smart contract*, in R. Battaglini, M.T. Giordano (a cura di), "Blockchain e smart contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche", Giuffrè, 2019

P. De Filippi, A. Wright (2018), *Blockchain and the Law. The Rule of Code*, Harvard University Press, 2018

M.C. Gaeta, L. Aulino, E. Troisi (2023), *The Possible Relationship Between Law and Ethics in the Context of Artificial Intelligence Regulation*, in "HUMANA.MENTE Journal of Philosophical Studies", vol. 16, 2023, n. 44

M. Giancaspro (2017), *Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective*, in "Computer Law & Security Review", vol. 33, 2017, n. 6

T. Hewa, M. Ylianttila, M. Liyanage (2021), *Survey on blockchain-based smart contracts: Applications, opportunities, and challenges*, in "Journal of Network and Computer Applications", vol. 177, 2021

P. Ibáñez Colomo (2021), *The draft Digital Markets Act: A legal and institutional analysis*, in "Journal of European Competition Law & Practice", vol. 12, 2021, n. 7

A.U. Janssen, F.P. Patti (2020), *Demistificare gli smart contracts*, in "Osservatorio del diritto civile e commerciale", 2020, n. 1

M. Marletta, F. Mastroianni (2024), *Balancing individual will and social benefit: a study of contract regulation*, in "Amministrativ@mente", 2024, n. 3

50. Sklaroff 2017.

V. Natalini (2011), *Il collegamento contrattuale, buona fede ed equilibrio tra i contratti*, in AMS Institutional Doctoral Theses Repository, 2011

A. Nicolussi, G. Portonera (2023), *Buona fede e correttezza nel rapporto obbligatorio*, in R. Alessi, G. Grisi, A. Nicolussi, G. Portonera, "Le obbligazioni", vol. IV - Trattato del Diritto Privato - Tomo I, Giappichelli, 2023

L. Piatti (2016), *Dal codice civile al codice binario:* blockchains *e* smart contracts, in "Ciberspazio e diritto", 2016, n. 3

M. Raskin (2017), *The Law and Legality of Smart Contracts*, in "Georgetown Law Technology Review", vol. 1, 2017, n. 2

A. Savelyev (2017), *Contract law 2.0: "Smart" contracts as the beginning of the end of classic contract law*, in "Information & Communications Technology Law", vol. 26, 2017, n. 2

F. Scolaro, M.L. Zannini Quirini (2020), *Gli aspetti eticizzanti della clausola di buona fede nella Relazione al Codice civile del 1942*, in "Sapienza Legal Papers", vol. 7, 2020

J.M. Sklaroff (2017), *Smart contracts and the cost of inflexibility*, in "University of Pennsylvania Law Review", vol. 166, 2017, n. 1

N. Szabo (1997), *Formalizing and Securing Relationships on Public Networks*, in "First monday", vol. 2, 1997, n. 9

H. Taherdoost (2023), *Smart contracts in blockchain technology: A critical review*, in "Information", vol. 14, 2023, n. 2

G. Teubner (2000), *Contracting worlds: the many autonomies of private law*, in "Social & Legal Studies", vol. 9, 2000, n. 3

E. Tosi (2021), *Diritto privato delle nuove tecnologie digitali. Riservatezza, contratti, responsabilità tra persona e mercato*, Giuffrè, 2021

E. Tosi (2010), *Contratti informatici, telematici e virtuali. Nuove forme e procedimenti formativi*, Giuffrè, 2010

A. Venturelli (2017), *Clausola di "hardship"*, in M. Confortini (a cura di), "Clausole negoziali. Profili teorici e applicativi di clausole tipiche e atipiche", Utet Giuridica, 2017

M. Vestoso (2021), *Diritto e tecnologia: una riflessione critica sui contenuti di un rapporto in continua evoluzione*, in "Teoria e Critica della Regolazione Sociale", vol. 2, 2021, n. 23

S. Wang, Y. Yuan, X. Wang et al. (2018), *An Overview of Smart Contract: Architecture, Applications, and Future Trends*, in "IEEE Intelligent Vehicles Symposium (IV)", IEEE, 2018

K. Werbach (2018), *Trust, but verify: Why the blockchain needs the law*, in "Berkeley Technology Law Journal", vol. 33, 2018, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0215 • articolo sottoposto a peer review • pubblicato in anteprima il 2 apr. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Paola D'Abbrunzo

Regolamento generale sulla protezione dei dati e cybersecurity nelle pubbliche amministrazioni: le nuove sfide, le opportunità e best practices delle istituzioni scolastiche, nel contesto delle risorse del PNRR

Il lavoro si propone di fornire un'analisi dell'intersezione tra il Regolamento generale sulla protezione dei dati personali (GDPR), e la cybersecurity nelle pubbliche amministrazioni. In particolare, il focus del contributo sarà incentrato sulle istituzioni scolastiche e sull'effettivo grado di applicazione della normativa in materia di trattamento dei dati, nel contesto post-pandemico di digitalizzazione e utilizzo di strumenti cloud, mettendo in luce le criticità quotidiane che le scuole vivono e le soluzioni auspicabili per trovare il giusto bilanciamento tra spinte digitali ed esigenza di tutelare tutti i diritti fondamentali in materia di privacy e riservatezza. La trattazione fornirà una prima valutazione sul come e quanto le iniziative e le risorse del PNRR, che mirano a rafforzare i servizi di gestione della minaccia cyber per la protezione dell'ecosistema digitale nazionale, impattino sull'opera di ammodernamento e aggiornamento delle infrastrutture digitali e di sicurezza informatica delle istituzioni scolastiche.

GDPR – Privacy – Istituzioni scolastiche – PNRR – Cybersecurity

General Data Protection Regulation and Cybersecurity in public administrations: the new challenges, opportunities and best practices of educational institutions, in the context of the PNRR resources

The work aims to provide an analysis of the intersection between the General Data Protection Regulation (GDPR), and cybersecurity in public administrations. In particular, the focus of the contribution will be on educational institutions and the actual degree of application of the data processing regulations, in the post-pandemic context of digitalization and use of cloud tools, highlighting the daily critical issues that schools experience and the desirable solutions to find the right balance between digital pressures and the need to protect all fundamental rights in terms of privacy and confidentiality. The discussion will provide an initial assessment of how and to what extent the initiatives and resources of the National Recovery and Resilience Plan, which aim to strengthen cyber threat management services for the protection of the national digital ecosystem, impact the modernization and updating interventions of digital infrastructures and cybersecurity of educational institutions.

GDPR – Privacy – Educational institutions – NRRP – Cybersecurity

L'Autrice, laureata in Giurisprudenza e specializzata in professioni legali, è dipendente del Ministero dell'Istruzione e del Merito, in qualità di Direttore dei servizi generali e amministrativi

Sommario: 1. Premessa: definizione del dato personale e suo trattamento, in particolare nel contesto delle istituzioni scolastiche. – 2. Le specificità del trattamento dei dati nelle scuole. La base giuridica, il ruolo del titolare e del responsabile del trattamento, le norme più rilevanti del GDPR in materia. – 3. Il ruolo fondamentale della formazione continua degli stakeholder per la corretta applicabilità del Regolamento. – 4. Gli attacchi cyber nelle istituzioni scolastiche: il "phishing" e "pharming". Gli strumenti per garantire la sicurezza informatica e l'apporto, sul punto, delle risorse del PNRR. Osservazioni conclusive.

1. Premessa: definizione del dato personale e suo trattamento, in particolare nel contesto delle istituzioni scolastiche

Stando alla sua definizione, il dato personale[1] rappresenta "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)" e il suo "trattamento"[2] è inteso come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione[3].

Il tema del trattamento del dato è particolarmente caldo, se si considera il contesto scolastico, posto che la maggior parte dei dati personali che ne costituiscono il database riguarda dati di minorenni e dati sensibili. Si pensi, ad esempio, a tutti i dati raccolti, nelle e dalle scuole, con riferimento agli alunni diversamente abili, per i quali, la loro gestione comporta il trattamento di documentazione medica, diagnosi, referti, decreti di invalidità. O anche ai dati giudiziari che possono essere oggetto di trattamento relativamente agli studenti, dati che rilevino le origini razziali ed etniche (possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri e in alcuni casi possono desumersi anche dai nominativi o dai dati anagrafici degli alunni) oppure le convinzioni religiose (per garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento). Siamo più che mai di fronte, quindi, al trattamento di dati sensibili e sensibilissimi[4], per i quali le scuole sono tenute a procedere solo nel rispetto e per quanto strettamente necessario al raggiungimento delle "finalità di istruzione e formazione".

In tale contesto, naturalmente, non va dimenticato che, insieme a tanti dati personali degli alunni, dati sensibili e, al limite, giudiziari, possono dover entrare in gioco anche nell'ambito dei rapporti di lavoro gestiti dagli enti scolastici con dirigenti, docenti e personale ATA. Il singolo istituto scolastico, sotto questo profilo, è, infatti, un ordinario datore di lavoro[5] che tratta i dati dei dipendenti per la gestione del rapporto lavorativo, nel rispetto

1. Per uno sguardo d'insieme, v. Belisario–Riccio–Scorza 2022.
2. Si veda D'Orazio–Finocchiaro–Pollicino–Resta 2021.
3. Cfr. artt. 4 e 7 del GDPR 2016/679.
4. Così Pizzetti 2021.
5. Sul punto, Pisani–Proia–Topo 2022.

delle norme che regolano tutte le sue fasi, dall'assunzione fino alla cessazione.

L'ambiente "scuola", dunque, è particolarmente complesso, sotto il profilo del trattamento dei dati personali e della tutela della privacy ed è questo il motivo per cui la sua regolamentazione è risultata spesso frastagliata e stratificata. Da questo punto di vista, la scelta del legislatore, di operare su un impianto normativo già esistente, innestando su di esso i nuovi obiettivi imposti dal GDPR, è risultata problematica: al netto di un innegabile miglioramento in termini di conoscibilità, circolazione, trattamento dei dati personali, ciò che si è ottenuto emendando il vecchio d.lgs. 196/2003 e il successivo d.lgs. 10 agosto 2018, n. 101, è, a parere di chi scrive, una eccessiva sovrapposizione tra gli istituti, incertezza sugli obblighi, indeterminatezza dei limiti.

2. Le specificità del trattamento dei dati nelle scuole. La base giuridica, il ruolo del titolare e del responsabile del trattamento, le norme più rilevanti del GDPR in materia

Proprio per questi motivi, e, data l'esigenza della protezione dei dati personali e della privacy[6], che nelle scuole è particolarmente rilevante, l'autorità di controllo, il Garante della privacy[7], nel 2023, ha sentito la necessità di aggiornare (alla luce del Regolamento UE 2016/679) e ampliare i contenuti già presenti nel vademecum del 2016, redigendo e pubblicando il nuovo vademecum 2023 dal titolo "La scuola a prova di privacy".

La revisione che viene richiesta dal GDPR, chiaramente richiamata nel vademecum, comincia dal novero dei soggetti coinvolti nel trattamento dei dati, dal momento che, al di là delle assonanze terminologiche, risultano profondamente incisi i ruoli e le responsabilità attribuiti a ciascuno di essi.

Alla luce di ciò, all'interno dell'organigramma dell'istituto scolastico, ogni scuola è tenuta così ad individuare le figure indicate dal GDPR e dal novellato Codice Privacy e che si possono così elencare:

- titolare del trattamento
- responsabili (esterni) del trattamento
- eventuali sub-responsabili
- responsabile della protezione dei dati

Il primo equivoco che va chiarito, per quanto possa suonare scontato agli esperti della materia, è che il titolare del trattamento, ossia il soggetto che determina le finalità e i mezzi del trattamento dei dati personali[8], sarà sempre l'istituto scolastico nel suo complesso e non già la persona fisica posta alla sua direzione, il cui ruolo sarà quello di dare esecuzione alle determinazioni del titolare. Nel nuovo quadro regolamentare, il titolare del trattamento è chiamato ad assicurare, attraverso scelte proprie, l'obiettivo del massimo grado di protezione dei dati trattati, facendosi guidare dal principio di accountability, o principio di responsabilizzazione, che, nella realtà dei fatti, si tradurrà, ad esempio, nell'accurata selezione dei soggetti cui affidare servizi e forniture. È proprio in relazione all'adeguatezza delle misure che si individua uno dei primi cambi di rotta rispetto alla normativa previgente. Il Codice Privacy, infatti, all'articolo 33 e nell'Allegato B, faceva riferimento ad una serie di misure minime – che tutti i titolari erano tenuti ad adottare – volte ad assicurare un livello basilare di protezione dei dati. Il legislatore europeo, invece, ben conscio dell'evoluzione e del progresso tecnologico ha spazzato via il requisito di misure "minime" prevedendo che i titolari adottino misure adeguate alla protezione dei dati in linea con la realtà in continuo mutamento. Conformemente a tale impostazione e in aderenza a tale inversione di tendenza, l'articolo 27, comma 1, lett. d), del d. lgs. n. 101/2018 ha abrogato proprio l'Allegato B del Codice Privacy.

Il legislatore nazionale, al novellato articolo 2 del d.lgs. 196/2003, ha, poi, previsto che, nell'ambito dell'organigramma organizzativo dell'istituto, specifici compiti e funzioni connessi al trattamento di dati personali siano demandati ad un ufficio o singolo dipendente, che però deve essere particolarmente qualificato e deve essere individuato con apposito atto di nomina. Quest'ultimo, può essere incaricato a coadiuvare la tenuta del registro delle

6. V. Relazione illustrativa riguardante "Disposizioni per l'adeguamento del Regolamento 2016/679 UE relativo alla protezione dei dati personali delle persone fisiche nonché alla loro libera circolazione, abrogazione della direttiva 95/46/CE", XVIII LEG - Schema di D.Lgs.
7. Sul ruolo del Garante, v. tra gli altri Busia–Ferola 2017.
8. Garante per la protezione dei dati personali 1997.

attività di trattamento[9], a coordinare l'attività di aggiornamento delle informative da rendere agli interessati[10] e a valutare i soggetti da nominare responsabili del trattamento[11].

Passando al responsabile del trattamento dei dati[12], questo è la persona fisica o giuridica, distinta dal titolare, che elabora dati per conto di quest'ultimo, sotto il suo controllo.

Requisito per la nomina è che il responsabile presenti garanzie sufficienti per mettere in atto opportune misure tecniche a tutela dei diritti degli interessati. Questa carica, che nelle scuole è svolta da un soggetto esterno, deve essere disciplinata da un contratto o da un atto giuridico, nel quale devono essere indicati i limiti e le istruzioni in merito al trattamento dei dati.

Una figura completamente nuova è, invece, quella del responsabile della protezione dei dati (RPD o, secondo l'acronimo inglese DPO – *Data Protection Officer*), la cui nomina è obbligatoria per tutte le autorità e gli organismi pubblici, dunque, anche per gli istituti scolastici pubblici: l'art. 37, par. 1, lett. a) del Regolamento prevede espressamente che "il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali". La medesima obbligatorietà non vale anche per gli istituti privati, sebbene appaia preferibile che anche tali soggetti vi procedano, tenuto conto delle specificità dei dati trattati, dei soggetti interessati (per lo più minori) e dei rischi connessi con le attività di trattamento[13].

A differenza del responsabile del trattamento, il responsabile della protezione dei dati può essere un soggetto sia interno che esterno all'istituto. Nel primo caso, la nomina andrà formalizzata con un atto di designazione e dovrà farsi particolare attenzione alla sussistenza, anche solo potenziale, di un conflitto d'interessi[14]. Qualora si opti per un soggetto esterno, l'istituto procederà invece a stipulare un contratto di servizio con la persona – fisica o giuridica – aggiudicataria della procedura selettiva, nella quale saranno indicati i requisiti di partecipazione, la durata e le caratteristiche di esecuzione della prestazione, anche in applicazione delle disposizioni del Codice dei contratti pubblici, d.lgs 36/2023. In ogni caso, sia esso interno o esterno, a seguito della nomina del responsabile del trattamento, e di qualsiasi variazione, i suoi dati di contatto dovranno essere comunicati, dal titolare al Garante, mediante la procedura telematica disponibile sul sito[15]. Questa disposizione mira a garantire che le autorità di controllo possano contattare il responsabile della protezione dei dati in modo facile e diretto[16].

Le funzioni "ibride" del responsabile riguardano soprattutto attività di consulenza, da fornire al titolare del trattamento, passando per la cura della formazione del personale, fino a sorvegliare l'osservanza della normativa, fornendo, quando richiesto, un parere in merito alle valutazioni d'impatto. Sul punto, si deve precisare che l'onere di assicurare il rispetto della normativa e la conformità delle

9. Cfr. GDPR 2016/679, art. 30.
10. *Ivi*, artt. 13 e 14.
11. *Ivi*, art. 28.
12. *Ivi*, artt. 28 e 29.
13. Così il Gruppo dei Garanti Ue (WP 29) approvava il 13 dicembre 2016 tre documenti con indicazioni e raccomandazioni su importanti novità del Regolamento 2016/679 sulla protezione dei dati; in particolare le Linee guida sul DPO specificano i requisiti soggettivi e oggettivi di questa figura, la cui designazione sarà obbligatoria per tutti i soggetti pubblici e per alcuni soggetti privati sulla base di criteri che il Gruppo ha chiarito nel documento. Nel documento vengono illustrate (anche attraverso esempi concreti) le competenze professionali e le garanzie di indipendenza e inamovibilità di cui il DPO deve godere nello svolgimento delle proprie attività di indirizzo e controllo all'interno dell'organizzazione del titolare.
14. Cfr. art. 38 del GDPR 2016/679.
15. V. sito del Garante per la protezione dei dati personali.
16. Per una visione d'insieme, v. Gruppo Articolo 29 2017-a, punto 2.6, in particolare, l'art. 37, par. 7 del Regolamento (UE) 2016/679 e l'art. 28, c. 4 del d.lgs. 18 maggio 2018, n. 51.

operazioni di trattamento al GDPR ricade comunque sempre sul titolare poiché il responsabile della protezione dei dati non risponde personalmente in caso di inosservanza del GDPR.

Quanto alla valutazione d'impatto, l'esecuzione di un DPIA (*Data Protection Impact Assessment*) è obbligatoria soltanto se è probabile che il trattamento "provochi un elevato rischio per i diritti e le libertà delle persone fisiche"[17]. Ciò è particolarmente rilevante quando viene introdotta una nuova tecnologia di elaborazione dati, specie se sensibili. Per questo motivo, nelle scuole, specie a seguito delle riforme imposte dal PNRR, che stanno comportando una vera e propria rivoluzione digitale con la migrazione al cloud di tutti gli applicativi gestionali e di lavoro[18], sembrerebbe assolutamente necessaria, almeno da questo momento in poi, la realizzazione del DPIA. Invero, ad oggi, tale pratica non è osservata in tutti gli istituti scolastici e sono pochi quelli in cui il titolare del trattamento (unico responsabile della valutazione d'impatto) procede alla o alle valutazioni per descrivere la necessità, la proporzionalità e i relativi rischi connessi al trattamento dei dati. Una DPIA, infatti, può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Sembra, però, che sul DPIA vi sia ancora un certo margine di discrezionalità in capo al titolare del trattamento nelle istituzioni scolastiche, anche perché le Linee guida[19] non contengono indicazioni specifiche su questo punto, a conferma che il loro contenuto e il loro obiettivo è essenzialmente procedurale. Eppure, il ricorso al DPIA dovrà iniziare ad essere costante, se ci si vuole allineare al contesto del GDPR, che, appunto, ribadisce la centralità del titolare in ordine alla valutazione dei trattamenti e alle misure da adottare per assicurare la loro compliance con le regole di protezione dei dati personali. In sostanza, la valutazione di rischio deve iniziare ad essere inteso come un processo e flusso costante e come una fase comunque necessaria per ogni trattamento e prima che il trattamento stesso inizi.

L'elasticità della interpretazione delle disposizioni sulla valutazione del rischio è, dunque, compensata dalla continua sottolineatura, peraltro supportata sia dall'art. 24, paragrafo 1, che dall'art. 35, paragrafo 11 del Regolamento, che, sia l'analisi dei rischi che il DPIA, inteso come individuazione delle misure necessarie, devono essere concepite come un processo costante e, continuamente, in rinnovamento. Una conferma, dunque, che il GDPR contiene una normativa molto elastica e, per questo, adattabile a ogni innovazione tecnologica che comporti appunto il trattamento di dati personali.

3. Il ruolo fondamentale della formazione continua degli stakeholder per la corretta applicabilità del Regolamento

Questo continuo "work in progress" che l'applicazione corretta del GDPR impone o imporrà alle scuole, è strettamente collegata a quell'attività di formazione del personale, a cui si faceva prima riferimento, e che il DPO dovrebbe curare. Arriviamo così, ad un punto nevralgico e dolente della trattazione. La formazione del personale rappresenta un altro importante milestone del PNRR. Le ultime due misure del PNRR, che stanno in questo momento interessando le scuole, introdotte, in Italia, con il d.m. 65/2023 e d.m. 66/2023 puntano, esclusivamente, all'aggiornamento e alla formazione del personale. Mentre il primo decreto, però, mira a formare i docenti delle scuole sulle discipline STEM e sul multilinguismo, il d.m. 66/2023 è la vera opportunità per le scuole per formare il proprio personale, specie quello che lavora nelle segreterie scolastiche, che ha a che fare tutti i giorni con

17. Cfr. art. 35, par. 1 del GDPR 2016/679 in base al quale "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".
18. V. Missione 1, Componente 1, investimento 1.2 del PNRR "Abilitazione al Cloud per le PA Locali - Scuole".
19. Cfr. Gruppo di lavoro Articolo 29 2017, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

tematiche quali la trasparenza e la sezione "amministrazione trasparente" dei siti web, il trattamento dei dati, la conservazione e l'archiviazione dei documenti, il rapporto con i dati sensibili degli alunni minori.

L'obiettivo è quello di sviluppare competenze digitali in linea con i quadri di riferimento europei DigComp 2.2 e DigCompEdu. La formazione, però, non potrà essere adeguata se non si considera che, allo stato attuale, il livello di preparazione delle segreterie scolastiche è basso o medio/basso e difficilmente performante rispetto ai nuovi adempimenti delle "scuole digitali". Si rileva, infatti, ancora molta superficialità nel trattamento dei dati personali, poca dimestichezza nel reperire in maniera corretta le informative, addirittura poca propensione dei titolari, ovvero degli istituti, a tener costantemente aggiornate le stesse, nel rispetto degli articoli 13 e 14 GDPR[20].

Partendo da tali considerazioni, sarebbe interessante monitorare, nel breve e medio periodo, come e se le scuole redigeranno informative non eccessivamente strutturate che potrebbero veder compromesso il requisito della chiarezza e della semplicità optando, invece, per una pluralità di informative ritagliate sulla categoria di interessati cui saranno dirette (alunni/famiglie da un lato, dipendenti dall'altro, fornitori etc.). La categoria degli interessati, ricordiamolo, nell'ambito degli istituti scolastici, è costituita perlopiù da soggetti minorenni che, dunque, non possono rilasciare alcun valido consenso al trattamento dei dati fino al compimento del diciottesimo anno di età[21]. Qualora, invece, lo studente dovesse raggiungere la maggiore età nel corso del ciclo scolastico sarà necessario acquisire il consenso direttamente dall'interessato e non dai genitori o dai soggetti che ne hanno precedentemente esercitato la responsabilità genitoriale.

Non è da sottovalutare, su questo punto specifico, il contesto socio-economico in cui la scuola opera. Contesti complessivamente più disagiati, scuole site in aree a rischio in termini di dispersione scolastica, aree periferiche, riscontrano sicuramente una maggiore difficoltà di reperimento delle informative da parte delle famiglie, a dimostrazione del fatto che, in generale, il trattamento dei dati può essere connesso ad aspetti socio/economici/culturali. Spesso risulta problematico far comprendere la base giuridica del trattamento, ovvero che il trattamento dei dati, nell'ambito della scuola, è strettamente necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, e che avviene solo in virtù di una norma di legge o, se ammesso dalla legge, di regolamento (art. 2 *ter* d.lgs. 101/2018) e per le categorie particolari di dati, indicati dall'art. 9 del GDPR, per motivi di interesse pubblico rilevante (art. 2 *sexies* d.lgs. 101/2018).

Un altro importante adempimento a cui spesso non viene data la giusta attenzione è la tenuta del registro delle attività di trattamento, secondo quanto previsto dall'art. 30 par. 1 del GDPR. Si tratta di un documento di censimento e analisi contenente le principali informazioni relative alle operazioni di trattamento effettuate, che si configura come una "fotografia" sullo stato attuale dei trattamenti posti in essere. Esso deve avere forma scritta, anche elettronica e deve essere sempre mantenuto aggiornato.

Per le istituzioni scolastiche, il Miur, con nota n. 877 del 3 agosto 2018, ha trasmesso uno schema di registro delle attività di trattamento, corredato da una guida operativa, per la compilazione dei campi individuati, ma anche per questo strumento, la sua utilizzazione è molto scarsa[22].

Sul grado di attuazione del GDPR, nelle istituzioni scolastiche, pertanto, si può concludere che

20. Sul punto, v. Garante per la protezione dei dati personali 2023-b: in particolare, parte II - L'attività svolta dal Garante - Punto 4. Il Garante e le amministrazioni pubbliche – Paragrafo 4.3. La protezione dei dati personali in ambito scolastico e universitario, p. 39.
21. Il legislatore nazionale, all'art. 2 *quinquies* del Codice Privacy, ha previsto che "Il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione" fattispecie che, allo stato, non sembra poter interessare il mondo della scuola.
22. Cfr. Garante per la protezione dei dati personali 2023-b e quanto evidenziato al sito Internet del GPDP, nella sezione dedicata alla Scuola.

la vera sfida sarà quella di rivedere l'organizzazione delle attività nel suo complesso, non semplicemente in termini formali – attraverso un adeguamento documentale – quanto, piuttosto, a realizzare una rivoluzione culturale all'interno di molte prassi[23]. E tale spinta può essere fornita, oggi, solo dal PNRR.

4. Gli attacchi cyber nelle istituzioni scolastiche: il "phishing" e "pharming". Gli strumenti per garantire la sicurezza informatica e l'apporto, sul punto, delle risorse del PNRR. Osservazioni conclusive

Ancora solo grazie alle risorse del PNRR, si potrà effettivamente parlare di implementazione dei sistemi e degli strumenti di prevenzione contro i cyber attacchi. In questo senso, la conoscenza di buone pratiche al fine di incrementare la sicurezza informatica è fondamentale per tutti, non solo per i lavoratori e i dipendenti della pubblica amministrazione a cui vengono rivolti gli sforzi maggiori. A maggior ragione, l'attenzione deve essere indirizzata a coloro che sono nella fase iniziale del loro corso di vita e che sono a rischio di incorrere in fenomeni quali la pedopornografia online, l'adescamento in rete, il cyberbullismo, la sextortion, la dipendenza patologica da Internet, l'estorsione di informazioni personali, come appunto possono essere i minori.

Cybersecurity nel contesto scolastico significa quindi due cose: da un lato, significa educare e promuovere un'alfabetizzazione digitale critica per i bambini e i ragazzi e guidare i genitori nell'uso di Internet da parte dei figli a casa; dall'altro, significa potenziare le infrastrutture digitali già esistenti nelle scuole o prevederne delle nuove, ma con adeguata preparazione e formazione di chi queste infrastrutture le deve gestire ed utilizzare. Se la trasformazione digitale affonda le proprie radici nei dati, è necessario che questi siano al sicuro e, per ottenere un simile risultato, non basta l'apporto tecnologico, soprattutto se non è inserito in un contesto di cultura della difesa e della sicurezza nel senso più ampio del termine. Il traguardo è ambizioso ma necessario e lo Stato italiano lo sa bene, tanto che il governo dell'allora premier Mario Draghi già approvava il d.l. 82/2021 con il quale, tra le altre cose, si è avuta la nascita dell'Agenzia per la cybersicurezza nazionale (ACN), di fatto operativa a partire dal mese di settembre del 2021.

I fondi del PNRR stanziati per la cybersicurezza ammontano a 623 milioni di euro: orbene, la parte più consistente, 301 milioni di euro, è destinata al potenziamento della resistenza cyber della PA, proprio per aumentarne la capacità di risposta, quindi reattività e non proattività[24]. I soldi stanziati (tra PNRR e ulteriori fondi deliberati dal governo) offrono una lettura che in linea di massima non ammette repliche: l'Italia si sta dotando delle infrastrutture per aumentare la propria resilienza agli attacchi cyber. Nonostante ciò, proprio per ricollegarci al quadro generale che si è cercato di fornire in questo lavoro, ben si può affermare che la sicurezza non è garantita soltanto dall'hardware e dal software, ma ha bisogno anche che lavoratori, studenti e cittadini siano più istruiti e formati, in modo da diventare più attenti. La cybersecurity deve essere un processo "aziendale" al pari degli altri e una dote che caratterizza i lavoratori, al pari delle conoscenze specifiche e tecniche relative alle professioni che svolgono.

Nel caso specifico delle scuole, diversi report[25]dimostrano, infatti, il notevole aumento degli attacchi ransomware nel comparto didattico,

23. Soro 2016, p. 20 ss., secondo cui si deve muovere alla ricerca di nuove e più efficaci forme di tutela delle nostre libertà, nel convincimento che la protezione dei dati personali rappresenta "la chiave attraverso cui è possibile ricercare il più alto punto di equilibrio tra uomo e tecnica".

24. Sul punto, v. Dipartimento per la trasformazione digitale 2022 e il programma di investimenti dell'Agenzia per la cybersicurezza nazionale, *Un programma di investimenti cybersecurity per un Paese ancora più sicuro*.

25. Cfr. Sophos 2022, Report dettagliato di studio annuale che ha coinvolto un totale di 730 professionisti IT dell'ambito didattico, che lavorano in aziende di medie dimensioni (100-5.000 dipendenti) distribuite fra 31 Paesi. Lo studio riporta la percentuale degli attacchi ransomware, i costi di ripristino e i livelli di copertura delle assicurazioni informatiche nel settore didattico. A causa dell'ampia varietà delle organizzazioni che operano nell'ambito didattico, il report fornisce dati separati per la scuola primaria o secondaria (fino a 18 anni) e per gli istituti universitari e parauniversitari (a partire dai 18 anni).

in questi ultimi anni, in cui gli operatori diventano spesso vittime inconsapevoli delle azioni di "phishing" e "pharming". Per phishing si intende quel tipo di attacco che consiste nell'inviare email malevole scritte appositamente con lo scopo di spingere gli utenti a rivelare informazioni bancarie, credenziali di accesso o altri dati sensibili; ciò avviene soprattutto quando le email sono "ben confezionate" e facilmente attribuibili a persone conosciute. Il termine pharming deriva invece dall'unione di "phishing" e "farming", e consiste in una metodologia in grado di dirottare il traffico internet verso server o siti gestiti dalla cybercriminalità, quindi non leciti, in modo da reperire tutte le informazioni e i dati personali ritenuti necessari ed "appetibili", perché essendo suscettibili di patrimonializzazione[26], e quindi di valutazione economica, ben si prestano alla loro commercializzazione indisciplinata, che pericolosamente, può diventare mercificazione.

Orbene, contrastare il phishing e il pharming non è facile, e tali fenomeni devono essere considerati come oggetto di formazione specifica e costante nel tempo. Su questi temi di cybersecurity, i programmi di sensibilizzazione del personale non possono avere un'efficacia permanente e devono essere ripetuti e aggiornati nel tempo (almeno una volta l'anno, meglio ancora semestralmente), se si considera l'alto grado di volatilità dei virus che, se reperiti e distrutti, vengono subito sostituiti da altri completamente nuovi.

Sarà importante e necessario, valutare, nel breve e medio periodo, quanti e quali scuole si adopereranno per includere la sicurezza informatica nell'offerta formativa degli alunni delle scuole primarie e secondarie, quante scuole prevedranno adeguati corsi di formazione per i dipendenti, quante faranno ricorso alla contrattualizzazione di un consulente esterno per gestire minacce e attacchi digitali.

Gli addetti ai lavori (AgID, Ministero per la Pubblica Amministrazione, Dipartimento per la Trasformazione Digitale) dovranno allora gettare le basi per l'elaborazione di uno studio, anche in un'ottica statistica, per rendicontare e dimostrare in che percentuale saranno effettivamente utilizzate nuove pratiche di miglioramento e prevenzione degli attacchi, quante applicheranno almeno le "misure minime" definite da AgID[27], l'Agenzia per l'Italia digitale, quanti dei soldi effettivamente stanziati verranno spesi per sviluppare competenze digitali in linea con i quadri di riferimento europei DigComp 2.2 e DigCompEdu e quanti per implementare le misure di Cybersecurity.

In fondo, sarò l'Unione europea a chiedercelo, nel momento in cui ci presenterà il conto per le risorse del PNRR concesse a favore dell'Italia.

Riferimenti bibliografici

AgID (2022), *Linee guida sull'accessibilità degli strumenti informatici dell'AgID*, 21 dicembre 2022

G. Alpa et al. (2021), *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

E. Belisario, G.M. Riccio, G. Scorza (a cura di) (2022), *GDPR e Normativa Privacy - Commentario*, IPSOA, 2022

F. Blefari, M. Paier, A.P. Paliotta (2023), *Educare alla sicurezza informatica: il ruolo delle scuole e del privato-sociale*, in "AgendaDigitale", 29 novembre 2023

L. Bolognini, E. Pelino (2024), *Codice della disciplina privacy*, Giuffrè, 2024

G. Busia, L. Ferola (2017), *Il Garante per la protezione dei dati personali. Le funzioni, i rapporti con le altre Istituzioni ed Autorità in Italia e in Europa*, in G. Busia, L. Liguori, O. Pollicino (a cura di), "Le nuove frontiere della privacy nelle tecnologie digitali", Aracne, 2017

26. Sentenza n. 2631/2021 del Consiglio di Stato.

27. Circolare n. 2 del 18 aprile 2017.

G. Carullo (2018), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa,* Giappichelli, 2018

R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) (2021), *Codice della privacy e data protection*, Giuffrè, 2021

Dipartimento per la trasformazione digitale (2022), *Cybersicurezza e resilienza per la trasformazione digitale della PA*, 2022

ENISA (2024), Implementing guidance. On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures, October 2024

Garante per la protezione dei dati personali (2023-a), *La Scuola a prova di privacy*, 2023

Garante per la protezione dei dati personali (2023-b), *Relazione annuale 2023*

Garante per la protezione dei dati personali (1997), *Titolare, responsabile, incaricato - Precisazioni sulla figura del "titolare"*, doc. web n. 39785, 9 dicembre 1997

Gruppo di lavoro Articolo 29 (2017), *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

Gruppo di lavoro Articolo 29 (2017-a), *Linee guida sui responsabili della protezione dei dati (RPD)*, 2017

C. Pisani, G. Proia, A. Topo (a cura di) (2022), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, 2022

F. Pizzetti (a cura di) (2021), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli, 2021

F. Pizzetti (2018), *Delega per il GDPR, i punti forti e deboli: un primo giudizio*, in "Agenda Digitale", 23 agosto 2018

Sophos (2022), *The State of Ransomware in Education 2022*, 21 luglio 2022

A. Soro (2016), *Liberi e connessi*, Codice, 2016

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0218 • articolo sottoposto a peer review • pubblicato in anteprima il 15 mag. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Alessandro Manfredi

I processi decisionali automatizzati nel GDPR, spunti e riflessioni interpretative

Il contributo analizza l'articolo 22 del GDPR, norma che tutela i soggetti da decisioni basate unicamente su processi automatizzati con effetti giuridici o analogamente significativi. L'indagine esamina la controversa natura della disposizione, interpretabile come divieto generale o diritto di opposizione, tenendo conto degli obiettivi perseguiti dal regolamento. Si evidenzia la distinzione definitoria tra processi decisionali automatizzati e profilazione *ex* articolo 4(4), configurandoli quali strumenti distinti seppur potenzialmente interconnessi. Particolare rilevanza assumono nella trattazione i criteri qualificanti gli effetti giuridici e gli effetti significativi, parametri determinanti per l'applicabilità della norma. Infine, la riflessione incorpora gli sviluppi giurisprudenziali comunitari, con riferimento alla sentenza C-634/21, concludendo sull'essenziale funzione equilibratrice della norma tra tutela dei diritti individuali e innovazione tecnologica.

GDPR – Articolo 22 – Processi decisionali automatizzati – SCHUFA – Accountability

Automated decision-making processes under the GDPR: insights and interpretative reflections

This paper examines Article 22 GDPR, which safeguards data subjects against solely automated decisions producing legal or similarly significant effects. The investigation interrogates the provision's contested normative characterization, prohibition versus right to object, contextualizing this interpretative dilemma within the regulation's teleological framework. The research delineates conceptual boundaries between automated decision-making processes and profiling operations under Article 4(4), establishing them as discrete regulatory constructs despite potential operational convergence. Critical attention focuses on definitional parameters qualifying "legal effects" and "significant effects" as applicability thresholds. The examination incorporates jurisprudential developments, particularly Case C-634/21, illuminating evolving judicial interpretations. The inquiry concludes by emphasizing Article 22's essential function in calibrating individual rights protection against technological innovation.

GDPR – Article 22 – Automatic decision-making systems – SCHUFA – Accountability

L'Autore è dottorando di ricerca in "Diritto della società digitale e dell'innovazione tecnologica" – Università Magna Græcia di Catanzaro

Sommario: 1. Introduzione. Essere umano e macchina. – 2. Articolo 22(1) del GDPR, tra divieto generale e diritto di opposizione. – 3. Il processo decisionale automatizzato e la profilazione, punti d'incontro e differenze. – 4. L'importanza degli effetti significativi nell'applicazione della norma. – 5. Il momento di automazione del processo decisionale. La sentenza C-634/21 - SCHUFA. – 6. Conclusioni.

1. Introduzione. Essere umano e macchina

L'integrazione dei sistemi di intelligenza artificiale (AI) negli apparati pubblici e privati è diventata prerogativa di ogni Stato industrializzato. L'AI, in quanto elemento cogente della nuova transizione tecnologica, coinvolge nel suo percorso evolutivo e integrativo un'ampia moltitudine di settori disciplinari: il diritto, la sociologia, l'ingegneria e finanche, la geopolitica[1].

L'AI attuale, spesso definita come "macchina", è ben lontana dai vecchi algoritmi utilizzati nei calcolatori, propri della prima società informatizzata[2], e le abilità in possesso dei vari software esistenti – ossia il compiere operazioni complesse in poco tempo, senza sforzi e con un alto livello di precisione – ne hanno consentito una rapida espansione. L'AI nelle sue moderne forme[3] presenta delle notevoli capacità di comprensione del linguaggio, tali da poter consentire una collocazione "spaziale" di parole e immagini nella sua infosfera. Antecedentemente all'introduzione delle versioni più moderne dei software di intelligenza artificiale, la collocazione spaziale delle informazioni non era particolarmente sviluppata, portando a evidenti problemi di natura semantica[4]. Nel semplificare l'argomento, basti pensare che i software

1. La corsa globale all'intelligenza artificiale è caratterizzata da quattro matrici principali: innovazione, capitale, regole e dati. A tali matrici conseguono pesanti implicazioni politiche e geopolitiche, e sono influenzate, da Stato a Stato, dalla quantità di risorse investite e dai diversi campi applicativi cui una nazione mira. Sulla dotazione globale di software AI, con particolare riguardo sulle prospettive europee v. Le Fevre Cervini 2024, Aa. V.v. 2022, Ricart–Álvarez-Aragonés 2023, Csernatoni 2024.
2. A questo proposito, autorevole dottrina si è occupata in passato dell'incidenza della tecnologia su quella che oggi può essere definita come una "primigenia" della società digitalizzata, ossia quando i software di intelligenza artificiale, come quelli odierni, erano difficili da immaginare. Con riguardo all'informazione automatizzata, è spesso stata percepita in dottrina l'esigenza di creare un diritto dell'informazione, al tempo non esistente, che si confrontasse con l'artificialità, intesa quale aspetto o momento dell'esperienza giuridica, al pari dell'etica. Così si esprime autorevole dottrina, sul punto v. Frosini 1968; Frosini 1992 il quale richiama a Bing 1981, Frosini 1984 e Roppo 1984, pp. 75 ss.; Borruso 1997.
3. Il riferimento è in particolare ai noti sistemi di machine learning, alle reti neurali e anche ai c.d. algoritmi genetici.
4. La capacità di un software di constatare la "distanza semantica" tra diversi vocaboli è importante, questa viene favorita dalle c.d. operazioni di *embedding*, consistenti nella possibilità di rappresentare dati complessi in uno spazio vettoriale. L'obiettivo principale delle operazioni di *embedding* è agevolare, in fase di apprendimento, la distinzione contestuale di vari elementi, con l'obiettivo di comprendere il contesto e dirimere eventuali dubbi o errori, come nei casi di ambiguità lessicale (ad esempio distinguere se una parola è un verbo o un pronome). In argomento v. Taher Pilehvar–Camacho-Collados 2021.

di intelligenza artificiale meno recenti non erano capaci di contestualizzare le parole, non riuscendo a distinguere, ad esempio, un oggetto da un marchio commerciale o da una persona.

Le suddette capacità di distinzione consentono ai software di poter etichettare con maggior precisione le informazioni che vengono loro affidate. Ed è proprio tale attività di *feeding* che consente al software AI di migliorare, portando addirittura alla fioritura di concrete capacità creative, in alcuni casi concorrenti con quelle umane[5], non apparendo più così lontana la prospettiva di un'AI sempre più autonoma rispetto all'essere umano. Sicché, è lecito domandarsi dove possa essere collocato l'essere umano quando relazionato al software e, soprattutto, se e quando questo debba investirsi dell'incarico di gestore, freno e supervisore delle operazioni svolte dalla macchina.

La collocazione dell'umano, del naturale che sovraintende l'artificiale, acquista particolare significato se rapportato alle problematiche inerenti all'uso dei dati personali da parte dei software AI. Come banalmente traspare dall'acronimo dei software GPT (*Generative Pre-trained Transformer*) di ampio utilizzo, il training del software è fondamentale ai fini di un corretto adempimento degli incarichi assegnati e questo dipende in larga parte dai dati che gli vengono forniti. Fornire informazioni in gran quantità, ma soprattutto fornire informazioni di qualità, permette al software di elaborare output sempre più complessi, garantendo addirittura la possibilità di elaborare output di carattere decisionale. Ed è su questo punto che dubbi e criticità etiche e giuridiche si incontrano.

La protezione delle informazioni fornite ai software di intelligenza artificiale, la soggezione o meno dei processi automatizzati al controllo umano e la possibilità di mantenere una certa flessibilità di utilizzo sono tutte criticità ascrivibili all'uso dei predetti software, soprattutto quando programmati per prendere delle decisioni i cui effetti ricadono sugli individui.

Per provare a dare una dimensione giuridica ai problemi fin qui esposti, è sicuramente necessario individuare quello che, allo stato attuale, è la norma principalmente preposta alla tutela dell'interessato dall'attività di trattamento dei dati personali[6] mediante *automatic decision making systems* (anche ADM o ADMS), soprattutto in assenza di un riscontro internazionale sul tema[7]. A riguardo, si fa riferimento all'articolo 22 del Regolamento UE 2016/679 *General Data Protection Regulation* (da qui in poi anche GDPR o Regolamento).

Il presente contributo è pertanto dedicato all'analisi delle principali sfide interpretative poste da tale articolo. In particolare, verrà esaminata: la dibattuta natura giuridica dell'articolo 22(1), quale divieto generale ovvero diritto di opposizione esercitabile dall'interessato; verranno approfonditi i requisiti applicativi fondamentali e verrà valutato l'impatto della recente giurisprudenza della Corte di Giustizia europea, la sentenza C-634/21 "SCHUFA", incidente sull'effettiva portata delle tutele predisposte dalla norma.

2. Articolo 22(1) del GDPR, tra divieto generale e diritto di opposizione

La *ratio* che caratterizza l'intero GDPR è tipizzata dal considerando 4 del Regolamento, ossia: "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo".

Pur in presenza di tale impostazione, è necessario tenere conto che il trattamento dei dati orientato al servizio dell'uomo, e la conseguente interpretazione umano-centrica del Regolamento, non corrisponde al riconoscimento della protezione dei dati personali quale prerogativa assoluta, dovendo intendersi, sempre secondo il considerando 4, in contemperanza con gli altri diritti fondamentali e in conformità con il principio di proporzionalità.

5. Hubert–Awa–Zabelina 2024.
6. La persona fisica identificata o identificabile cui i dati personali (*ex* articolo 4(1) del GDPR) si riferiscono.
7. Di Francesco Maesa 2022. Escludendo quanto prescritto dal diritto derivato, non è attualmente presente un atto giuridico internazionale vincolante ai fini della protezione degli individui soggetti a processi decisionali automatizzati, in particolare alla profilazione. Pur esistendo atti non vincolanti a riguardo (ad esempio, la Raccomandazione CM/Rec(2021)8 del Consiglio d'Europa "*On the protection of individuals with regard to automatic processing of personal data in the context of profiling*"), utili a delineare le varie criticità, questi non sono sufficienti a deframmentare il quadro giuridico internazionale.

La suddetta impostazione non si riflette soltanto sul continuo bilanciamento, in tema di AI, tra segreto industriale e trasparenza[8], ma sul complesso dettame dell'articolo 22 nella sua interezza[9].

Il testo dell'articolo 22(1) recita: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".

Analizzando gli elementi presenti nel testo della norma, il primo nodo da sciogliere riguarda la natura dell'articolo 22 stesso, ossia se questo realizzi un divieto di carattere generale o un diritto di opposizione in capo all'interessato dal trattamento. Partendo dalla collocazione della norma, il Legislatore comunitario ha collocato l'articolo 22 nella Sezione IV del Capo III del Regolamento, dei "Diritti dell'interessato", per cui di primo impatto, stando al dato letterale e alla collocazione della norma, il GDPR alluderebbe all'esistenza di un diritto di opposizione in capo all'interessato. È da specificare comunque che il GDPR nell'interezza della sua struttura propone diversi esempi di "attribuzione indiretta" di diritti. Ciò avviene generalmente attraverso la creazione di elenchi di adempimenti in capo al titolare del trattamento, dai quali derivano diritti per il soggetto interessato (si pensi alle formulazioni degli articoli 13 e 14 sul diritto di informazione) non espressamente tipizzati come tali; come avviene in altri punti dell'articolo 22[10] (in particolare al paragrafo 3)[11].

Inoltre, nel menzionare nuovamente il dettato del GDPR, l'articolo 13(2)(f) (come anche gli articoli 14(2)(g) e 15(1)(h)) sembra presupporre l'esistenza dell'articolo 22(1) quale diritto[12]. L'articolo 13(2)(f) menziona l'obbligo per il titolare di informare l'interessato, una volta ottenuti i suoi dati personali, circa l'esistenza di un processo decisionale automatizzato, al fine di garantire un trattamento corretto e trasparente; di conseguenza, ciò potrebbe consentire all'interessato l'esercizio di un

8. In particolare, al fine di "aprire" le c.d. black box. Bayamlioğlu 2023, pp. 330-332.
9. Mendoza–Bygrave 2017. Il necessario contemperamento tra diritti è altresì desumibile dal testo del considerando 71, nel quale viene rimarcata la possibile confluenza di errori nella decisione, le cui conseguenze potrebbero essere pregiudizievoli, su vari livelli, per l'interessato: "Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato … è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato…". I timori palesati dal Legislatore comunitario per mezzo del considerando 71, circa la qualità e gli errori presenti nelle decisioni automatizzate, erano già presenti nella *ratio* costitutiva dell'articolo 15 della proposta antecedente alla Direttiva 95/46/CE, o *Data Protection Directive* (DPD), nella quale la Commissione europea evidenziava il timore di un'assuefazione dell'interessato alle decisioni infallibili delle macchine: "Il rischio insito in un'utilizzazione abusiva dell'informatica in un processo decisionale rappresenta uno dei pericoli fondamentali per il futuro: infatti il risultato fornito dalla macchina che si avvale di software sempre più sofisticati oppure di sistemi esperti riveste un carattere apparentemente obiettivo e incontestabile a cui l'uomo, in qualità di responsabile della decisione, può accordare un'importanza eccessiva rinunciando alla propria responsabilità". COM (92) 422 – SYN 287, p. 27.
10. Tosoni 2021.
11. Articolo 22(3) del GDPR: "Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".
12. Bygrave 2020. Altresì, Tosoni individua come gli articoli 13(2)(f), 14(2)(g) e 15(1)(h), riferendosi all'articolo 22 per intero, presentino delle ridondanze in termini di trasparenza, soprattutto in relazione all'articolo 22(4) relativo ai divieti sul trattamento dei dati particolari. Inoltre, lo stesso Tosoni individua come in interpretazione analogica la Direttiva 680/2016, relativa al trattamento dei dati per finalità di *law enforcing*, si riferisca agli *automatic decision making systems* per mezzo di un divieto di portata generale. Per approfondimenti v. Tosoni 2021.

eventuale diritto di opposizione, sulla carta, nelle forme di una tutela *ex ante* rispetto alla decisione, ma concretamente difficile da esperire come tale.

Se sul piano letterale traspare un diritto esercitabile dall'interessato al fine di opporsi alle pratiche di *automatic decision making*, d'altra parte si tende a considerare la norma un divieto di carattere generale[13]; entrambe le ipotesi trovano sostegno in dottrina[14].

Infatti, qualora l'articolo 22(1) venisse considerato come un diritto di opposizione, il soggetto interessato dal trattamento dovrebbe personalmente attivarsi per opporsi al processo decisionale automatizzato. L'impostazione proposta porterebbe a un ridimensionamento della tutela offerta dall'articolo 22, in quanto l'interessato potrebbe non opporsi al processo decisionale, di conseguenza consentendolo[15].

Quanto testé prospettato implicherebbe quattro diverse eventualità: l'interessato si oppone al processo decisionale portando il titolare a optare per una decisione umana eliminando il "momento" automatico dal processo decisionale (sempre che la struttura algoritmica consenta all'essere umano di intervenire); l'interessato si oppone e il processo decisionale automatizzato viene bloccato in quanto non rientrante nelle eventualità di cui all'articolo 22(2)[16]; il processo decisionale è consentito in quanto rientrante nelle maglie dell'articolo 22(2); ultima eventualità, l'interessato non si oppone al processo decisionale[17].

Le eventualità sopra delineate andrebbero a concretizzarsi, *ex* articolo 12(3) del GDPR, in obblighi di natura procedurale in capo al titolare del trattamento, il quale, in approccio reattivo, dovrà tempestivamente ottemperare alla richiesta dell'interessato nell'arco temporale massimo di un mese (prorogabile a due mesi per richieste di particolare complessità)[18].

Come accennato, è possibile altresì considerare la norma un divieto di carattere generale. Nel seguire tale seconda linea interpretativa è apprezzabile il contributo di autorevole dottrina[19], la quale propugna un'interpretazione sistematica e meno restrittiva dei presupposti applicativi dell'articolo 22, lettura che, indirettamente, conforta la tesi del divieto generale quale regola di base. Si sostiene, ad esempio, che il requisito della decisione basata unicamente sul trattamento automatizzato non possa essere eluso mediante l'introduzione di interventi umani meramente formali o fittizi (il c.d. *rubber-stamping*). Tale approccio ermeneutico, ampliando la portata potenziale della fattispecie di cui all'articolo 22(1), ne rafforza la funzione protettiva intrinseca offrendo, secondo gli autori, maggiore certezza del diritto ai titolari operanti in un contesto normativo complesso.

Da questo punto di vista, è riscontrabile come un divieto di carattere generale risulti maggiormente idoneo a garantire le tutele della norma rispetto a un diritto di opposizione, mitigando *ab origine* eventuali interventi formali. Inoltre, la considerazione dell'articolo 22(1) quale divieto andrebbe ad armonizzarsi con la *ratio* complessiva del Regolamento[20], tesa a restituire all'individuo un controllo effettivo sui propri dati personali, in linea con la moderna considerazione della *data protection* quale gestione del patrimonio informativo dell'interessato[21].

13. Article 29 Data Protection Working Party 2017. Sul punto v. Brkan 2019.
14. Bygrave 2019, p. 7 ss.
15. Brkan 2019.
16. Quando il processo decisionale automatizzato *ex* articolo 22(2) è: necessario alla conclusione o all'esecuzione di un contratto tra l'interessato e un titolare del trattamento; è autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; è conseguenza del consenso esplicito dell'interessato.
17. Brkan 2019.
18. Caia–Iraci–Gambazza 2022.
19. Malgieri–Comandé 2017.
20. Kaminski 2019.
21. L'espressione è di Stefano Rodotà ed è riportata in Pascuzzi 2016, p. 47. Impostazione condivisa da recente giurisprudenza della Corte di Cassazione, che, in Cass., 27 marzo 2020, n. 7559, individua nella protezione dei dati personali "il diritto al potere dell'interessato di controllare consapevolmente i propri dati".

Un divieto di portata generale garantirebbe in sé una protezione intrinseca e automatica *ex ante*, prescindendo dall'attivazione specifica da parte dell'interessato – il quale potrebbe non essere consapevole di essere oggetto di processi decisionali automatizzati, o comunque, potrebbe non disporre degli strumenti o delle conoscenze idonee ad esercitare efficacemente un eventuale diritto di opposizione – e dalla conseguente "reazione" del titolare alla richiesta.

A favore del divieto si è espresso anche il *Working Party ex* Articolo 29 (ora *European Data Protection Board*), ossia l'organismo consultivo composto dai rappresentanti delle varie autorità nazionali, dal Garante europeo e da un rappresentante della Commissione Europea. Il Gruppo dei Garanti, nel cercare di dipanare i dubbi sulla natura dell'articolo 22(1), ha deciso di affrontare il problema attraverso un approccio puramente logico. Il ragionamento del Gruppo dei Garanti europei, contenuto nel parere WP251 "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", ruota attorno al rapporto intercorrente tra il primo paragrafo dell'articolo 22 e le deroghe all'applicazione dello stesso previste nel secondo, sintetizzabili nella strumentalità del trattamento: alla conclusione o esecuzione di un contratto tra l'interessato e il titolare (lett. a); al diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (lett. b); al consenso esplicito dell'interessato (lett. c).

Il Gruppo dei Garanti articola una posizione fondata sull'incoerenza che potrebbe emergere dalla contemporanea coesistenza di un diritto di opposizione con un trattamento dati legittimato attraverso il consenso dell'interessato. Tale antinomia si manifesterebbe nella difficoltà di conciliare due istituti giuridici che operano in direzioni funzionalmente opposte: da un lato, la manifestazione esplicita di volontà che autorizza il trattamento mediante consenso; dall'altro, l'esercizio di un diritto di opposizione che presupporrebbe l'esistenza di un trattamento fondato su basi giuridiche diverse dal consenso stesso. L'argomentazione dei Garanti evidenzia come la suddetta configurazione normativa risulti carente in termini logico-applicativi, generando così un'incoerenza sistemica[22].

A conferma della lettura dell'articolo 22 orientata al divieto, depone la stessa formulazione del considerando 71 – laddove afferma che "è opportuno che sia consentito" adottare decisioni automatizzate a determinate condizioni – che presupporrebbe una regola generale di segno opposto, ossia un divieto, rispetto alla quale le ipotesi delineate nel secondo paragrafo costituiscono deroghe espresse.

A riguardo, giova evidenziare come il GDPR sia stato concepito al fine di instaurare un approccio proattivo da parte del titolare del trattamento, incentrato sull'*accountability* e sulla flessibilità normativa[23]. Il GDPR ha aperto con decisione l'Europa a percorsi di governance collaborativa, attraverso, ad esempio, l'introduzione della privacy *by design*, la privacy *by default*[24] e la *Data protection impact assesment* (DPIA)[25]. I predetti istituti mirano a una protezione *ex ante* dell'interessato, concepita per adattare il trattamento dei dati agli oneri posti dal

22. Article 29 Data Protection Working Party 2017.

23. Pizzetti 2016, pp. 45-47.

24. Ideati in Canada, i principi di *privacy by design* e *by default* sono stati introdotti ad opera di Ann Cavoukian, Privacy Commissioner dell'Ontario, basandosi sulla mitigazione di eventuali futuri problemi attraverso un'opera di prevenzione sin dalla progettazione e su un buon livello di sicurezza per impostazione predefinita. Tali principi sono stati assorbiti e adattati al contesto normativo europeo per mezzo del GDPR, in quanto considerati tra le *best practices* a livello internazionale. Sul tema v. Cavoukian–Taylor–Abrams 2010; D'Aquisto–Naldi 2017, p. 33 ss; Pisapia 2018, pp. 101 e ss.

25. Bygrave 2020. Bygrave opportunamente evidenzia come il dettato dell'articolo 22 debba essere interpretato alla luce dell'articolo 35 relativo alla *data protection impact assessment*, la procedura introdotta dal GPDR che mira a descrivere un trattamento di dati personali al fine di valutarne la necessità, la proporzionalità e i relativi rischi, con il fine di approntare misure idonee ad affrontarli. La DPIA, in particolare per richiamo all'articolo 35(3)(a), è richiesta per i trattamenti in cui è prevista: "una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche". La predisposizione di una DPIA provvederebbe a garantire una protezione *ex ante* dell'interessato e quindi

Regolamento attraverso le c.d. operazioni di *compliance*, ossia le operazioni di uniformazione alle disposizioni normative. Il divieto si collocherebbe, da un punto di vista sistemico, in rapporto contiguo non solo con l'approccio per *accountability*, ma anche con le forme di tutela *ex post* previste dal GDPR, quali i ricorsi alle autorità di controllo e le notifiche agli interessati[26].

In sintesi, tenuto conto dei vari elementi emersi, il divieto non andrebbe a precludere in modo assoluto il ricorso ai processi decisionali automatizzati, ma andrebbe a circoscriverne la legittimità operativa a specifiche situazioni, scandite dal secondo paragrafo, imponendo, in aggiunta, un regime rafforzato di garanzie procedurali, individuabili nel dettato dell'articolo 22(3). Infatti, laddove operino le eccezioni di cui alle lettere a) e c), sorgerebbe in capo al titolare del trattamento l'obbligo imperativo di implementazione "di misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi", dovendo assicurare almeno il diritto dell'interessato a esprimere la propria opinione, a ottenere un intervento umano e a contestare la decisione presa[27]. Da un punto di visto procedurale, è utile considerare come al variare della natura dell'articolo 22(1) varierebbero le peculiarità applicative dell'articolo 12(3) del GDPR precedentemente menzionato. Il decorso dei termini dell'articolo 12(3) si sposterebbe dal momento di ricezione formale dell'istanza oppositiva dell'interessato al momento di concretizzazione della contestazione della presunta violazione del divieto, ovvero della richiesta di informazioni sul processo decisionale automatizzato, generando ulteriori difficoltà interpretative in relazione, in questo caso, al diritto di informazione e all'onere probatorio *ex* articolo 82 del GDPR.

3. Il processo decisionale automatizzato e la profilazione, punti d'incontro e differenze

Sin dalla rubrica dell'articolo 22, ossia "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione", il GDPR offre informazioni sulla natura di tali processi. Oltre a sottolineare la centralità della persona fisica, la rubrica rimarca la possibile natura della profilazione[28] quale processo decisionale automatizzato. Quanto indicato è marcatamente orientativo. Infatti, il Regolamento, oltre a elevare la profilazione quale processo equivalente o elemento di un ADM (e non mera forma di trattamento), ne segna l'importanza definitoria, collocando di fatto

antecedente alla decisione dell'ADMS, in particolare nel caso in cui venga consultata preventivamente l'autorità di controllo nazionale *ex* articolo 36 del GDPR. Di importante considerazione è come la DPIA sia conseguenza dell'*accountability* introdotta per mezzo del GDPR, la quale trova genesi nella, sempre più utilizzata, c.d. *collaborative governance*, ossia nella collaborazione sincrona tra entità pubbliche e private. Da un punto di vista normativo tale collaborazione si estrinseca in una sorta di responsabilizzazione dei privati a delle regole stabilite dall'autorità, le quali non sono imposte con rigidità (approccio statico o *top-down*, come avveniva con la Direttiva 95/46) da parte degli apparati di governo, consentendo controlli all'uopo successivi alla fase di *compliance*. Sul punto v. Kaminski–Malgieri 2021.

26. Cfr. D'Acquisto–Trovato–Benedetti 2022, pp. 345-347.

27. È stato oggetto di attenzioni in dottrina l'eventuale tenuità del diritto all'intervento umano, poiché, come accennato, potrebbe eccedere in formalità, precludendo, paradossalmente, tutele più forti se la decisione cessasse di essere unicamente automatizzata. Ben più pregnante è il diritto a contestare la decisione. Interpretato in dottrina non quale mera richiesta di riesame, bensì come un diritto procedurale che attiva un vero contraddittorio dialettico, ispirato alla *contestatio* giuridica. Questo obbliga il titolare a creare meccanismi interni equi per gestire la disputa (i menzionati diritti ad essere ascoltati, alla prova, a una decisione imparziale). Pur operanti su livelli differenti, tali diritti formano una progressione di tutele con la contestazione al vertice. Essa, per essere efficace, presuppone la possibilità di esprimere opinioni argomentate e, implicitamente, di ottenere spiegazioni adeguate sulla decisione, superando la lettura minimalista delle garanzie dell'articolo 22 GDPR. Sul punto v. Sarra 2020, pp. 1-12.

28. Intesa nella sua forma automatizzata quale processo che, una volta avviato, prosegue con un minimo intervento umano e le cui susseguenti decisioni sono prese autonomamente dal software/macchina, v. Ruggieri 2022, il quale richiama a Hildebrandt 2008.

l'unico processo automatizzato provvisto di descrizione a metro di paragone per un'intera categoria di processi, siano essi decisionali o no.

L'analisi della definizione di profilazione consente di individuare i margini operativi dell'articolo 22 e il novero degli elementi caratteristici dei processi decisionali automatizzati ricadenti nella norma.

La profilazione viene descritta dall'articolo 4(4) del GDPR come una forma di trattamento dei dati personali automatizzata, il cui fine è la valutazione di determinati aspetti personali afferenti a una persona fisica[29]. Per cui le tre caratteristiche principali delle attività di profilazione sono rintracciabili: nell'automazione del processo stesso, nell'uso dei dati personali e nella valutazione di aspetti afferenti alle persone fisiche[30].

Il confronto tra la definizione di profilazione fornita dall'articolo 4(4) e il testo dell'articolo 22(1)[31] del GDPR consente di individuare alcune delle caratteristiche di un generico processo decisionale automatizzato. Il processo decisionale *ex* articolo 22(1) presenta le seguenti caratteristiche: deve essere totalmente automatizzato, deve essere presa una decisione, la decisione deve produrre effetti giuridici o effetti significativi sulla persona cui è rivolta; inoltre è di curiosa constatazione la mancata presenza di una menzione del dato personale.

Su tali basi è possibile proporre alcune considerazioni. La totale automazione del processo decisionale è caratterizzante rispetto alla profilazione, giacché pur essendo qualificata dall'articolo 4(4) quale processo automatizzato, la profilazione non è necessariamente interamente automatizzata[32]. Tale considerazione giustificherebbe la collocazione della profilazione sia nella rubrica che nel testo dell'articolo 22 quale elemento compreso, ma non necessario, ai fini della norma, in quanto, la profilazione potrebbe diventare un processo totalmente automatizzato, a seconda delle circostanze di trattamento, ma non necessariamente esserlo[33]. A tal riguardo, è da prendere in esame il testo del considerando 71 del Regolamento, che, nel secondo paragrafo[34], sembrerebbe riferirsi alla profilazione come un elemento necessario di un processo decisionale automatizzato[35]. Questa considerazione è in linea con le realtà di trattamento dei dati per mezzo di ADMS, nei quali, nella maggior parte di casi, viene fatto ampio uso di tecniche

29. Articolo 4(4) del GDPR: "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".
30. In quanto strumento funzionale all'assunzione di una decisione rilevante per l'individuo o per il gruppo soggetto ad essa, in quanto mezzo adeguato a valutare e prevedere analiticamente il comportamento presente e futuro del soggetto profilato, sul punto v. Calzolaio 2017.
31. Qui nuovamente menzionato per comodità di raffronto: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".
32. Article 29 Data Protection Working Party 2017: "Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition".
33. *Ibidem*. Di fatto portando a tre diversi utilizzi della profilazione: raccolta dati (anche non automatizzata), decisioni basate sulla profilazione, decisioni totalmente automatizzate.
34. Considerando 71 del GDPR: "Tale trattamento comprende la 'profilazione', che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
35. Sartor–Lagioia 2020, pp. 59-60.

di profilazione[36]. Altresì, è da constatare come il medesimo considerando, nel paragrafo successivo, si riferisca alla profilazione quale processo a sé stante rispetto alla categoria degli ADMS[37], lasciando nell'opera di interpretazione alcuni dubbi[38]. Rientrando sugli articoli 4(4) e 22(1), un altro elemento fondamentale individuabile dall'analisi delle due definizioni, è l'assenza del dato personale dalle previsioni dell'articolo 22(1). Mentre la profilazione opera esclusivamente attraverso il trattamento di dati personali, in quanto è una forma di trattamento dei dati, i processi decisionali automatizzati descritti dall'articolo 22 non sono vincolati al solo utilizzo dei suddetti dati[39]; tale differenza tra le due eventualità è rintracciabile nella collocazione assunta dalla decisione all'interno dell'intero processo automatizzato. Infatti, la decisione è considerabile come lo *step* finale di un processo di elaborazione automatico, soprattutto mediante l'uso di software AI[40], che può essere conseguenza dei dati raccolti in precedenza, anche da altri soggetti[41].

Nel riassumere, è evidente come la profilazione sia assimilabile a una forma di trattamento dei dati personali volta alla creazione di *cluster*/profili di persone fisiche, mentre il processo decisionale automatizzato punta all'elaborazione di una decisione significativa per l'individuo cui è diretta, prescindendo dalla creazione di un profilo. Per cui, la profilazione potrebbe divenire un processo decisionale automatizzato qualora, mediante l'uso di strumenti di automazione (non necessariamente di intelligenza artificiale), venga presa una decisione conseguenziale alla profilazione stessa. Viceversa, un processo decisionale automatizzato può avvalersi di dati personali o misti, raccolti anche mediante profilazione, al fine di elaborare un output decisionale in forma automatica. È evidente come assuma fondamentale importanza ai fini dell'applicazione della norma, come si avrà modo di analizzare[42], l'individuazione del momento di automazione.

4. L'importanza degli effetti significativi nell'applicazione della norma.

Tra gli elementi necessari all'applicazione dell'articolo 22 meritano eguale attenzione gli effetti scaturenti dal processo decisionale automatizzato, anch'essi contraddistinti dalla mancanza di una precisa definizione. Infatti, gli elementi dell'articolo 22(1), nelle loro oscurità interpretative, sono caratterizzati da diverse gradazioni di individuabilità, con gli effetti prodotti dai processi decisionali automatizzati che risultano particolarmente difficili da individuare rispetto agli altri.

Al fine di suffragare tale affermazione, è necessario stabilire cosa intenda il GDPR per effetti significativi per l'interessato. L'articolo 22, come

36. Bygrave 2020.
37. Considerando 71 del GDPR: "Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore"..
38. Sul punto, come si avrà modo di illustrare in seguito, l'Avvocato Generale della Corte di Giustizia europea in relazione alla recente sentenza C-634/21, c.d. SCHUFA, ha asserito al punto 33 della sua disamina, come la profilazione, testo del Regolamento alla mano, possa essere considerata come una sub-categoria dei processi decisionali automatizzati.
39. Article 29 Data Protection Working Party 2017.
40. Determann 2024.
41. Article 29 Data Protection Working Party 2017.
42. *Infra* par. 5.

già descritto, afferma che il processo decisionale automatizzato debba necessariamente produrre effetti giuridici o un'incidenza analoga e significativa verso l'interessato dall'attività di trattamento. Gli effetti giuridici descritti dalla norma possono essere considerati alla stregua di attività di elaborazione impattanti non solo sui diritti degli interessati, ma anche sul loro status giuridico e su eventuali diritti scaturenti da un contratto[43], per cui di agevole individuazione.

Differentemente, gli effetti analoghi e significativi risultano più difficili da individuare, in quanto ricadenti in un insieme di eventualità meno marcato e di ampia portata. Nel provare a descrivere quali possano essere tali effetti, si può da subito constatare una differente impostazione dell'apparato regolamentare del GDPR rispetto alla Direttiva 95/46/CE.

La Direttiva 95/46/CE, c.d. *Data Protection Directive*, individuava all'articolo 15 il diritto dell'interessato a non essere sottoposto a una decisione esclusivamente automatizzata capace di produrre effetti giuridici o effetti significativi nei suoi confronti[44]. Al netto della parziale condivisione della *ratio*, e anche del testo[45], dell'articolo 15(1) della DPD con l'attuale formulazione dell'articolo 22(1) del GDPR (nel quale la Commissione europea palesava le prime perplessità e i primi timori rispetto a tali tipologie di processi[46]), l'articolo 15 mancava nella sua formulazione del termine "analogo". L'introduzione del termine "analogo" nell'articolo 22 del GDPR accresce di molto il campo di applicazione della norma rispetto all'articolo 15(1) della Direttiva 95/46[47]. L'introduzione di un'esplicita analogia descrittiva ha funzione di collegamento, creando un punto di incontro e rendendo gli effetti analoghi e significativi equivalenti agli effetti giuridici nelle loro implicazioni[48], pur non ricadendo in tale dimensione disciplinare.

Per cercare di circoscrivere la natura degli effetti analoghi e significativi, il *Working Party ex* Articolo 29 (da qui indicato anche come "Gruppo") ha individuato alcuni criteri di equivalenza circa l'impatto che tali effetti potrebbero avere sull'interessato, questi sono: l'incidenza significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato, la manifestazione di un impatto prolungato o permanente sull'interessato, l'esclusione o la discriminazione delle persone[49].

Seppur utili e indicativi, i criteri descritti dal *Working Party* non sono, per stessa affermazione del gruppo, sufficienti a quantificare con precisione la soglia oltre la quale gli effetti risultino talmente significativi da consentire l'applicazione dell'articolo 22, proponendo comunque alcune categorie di effetti nei quali tale soglia potrebbe essere superata[50].

Oltre a tali prospettive, il *Working Party* ha rivolto la sua attenzione anche all'eventualità in cui venga presa una decisione a seguito di un'esposizione a pubblicità online. È utile descrivere l'eventualità analizzata dal Gruppo, poiché l'*online advertising*

43. Ad esempio, il WP29 individua tra gli effetti giuridici: la possibilità di intraprendere azioni legali, di votare o la libertà di associazione, la cancellazione di un contratto, il diniego della cittadinanza. Article 29 Data Protection Working Party 2017, p. 21.
44. Articolo 15(1) Direttiva 95/46/CE: "Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.".
45. Oltre ad alcuni elementi presenti nei parr. 2 e 3 dell'articolo 22, tra i quali la deroga per prestazione del consenso e il diritto a ricevere un intervento umano. Wachter–Mittelstadt–Floridi 2017, pp. 81-82.
46. *Supra* nota 9.
47. Bygrave 2017.
48. Bygrave 2020.
49. Article 29 Data Protection Working Party 2017, pp. 21-24.
50. Decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito; decisioni che influenzano l'accesso di una persona ai servizi sanitari; decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

mirato è *una delle pratiche* di trattamento che fa maggior utilizzo degli strumenti di profilazione e, soprattutto, può essere considerata come la forma di trattamento da cui potrebbero manifestarsi la maggior parte degli effetti analoghi e significativi. Infatti, secondo il Gruppo, l'*online advertising* mirato potrebbe non essere significativamente incidente su tutti i nuclei di individui possibili, in quanto non tutte le attività pubblicitarie di questo tipo portano gli utenti a compiere decisioni significative. Per tale motivo nel parere WP251 sono stati elencati alcuni fattori che consentirebbero di rubricare i singoli casi di trattamento, fornendo di fatto ulteriori criteri di valutazione circa l'esistenza o meno di effetti significativi *ex* articolo 22. L'invasività del processo, le aspettative delle persone interessate e lo sfruttamento della conoscenza delle vulnerabilità degli utenti sono tutti elementi che, secondo il *Working Party*, consentirebbero l'individuazione di effetti significativi scaturenti da una decisione (in questo caso presa per mezzo di strumenti pubblicitari)[51]. Anche in questo caso i parametri forniti dal gruppo, seppur indicativi, non sono sufficienti a delineare con totale precisione il campo operativo dell'articolo 22[52].

5. Il momento di automazione del processo decisionale. La sentenza C-634/21 - SCHUFA

Nei districati anfratti dell'articolo 22, alla già complessa identificazione della norma e alla difficile delimitazione degli effetti incidenti sull'interessato, si affiancano discreti dubbi sul momento di automazione del processo decisionale. Se identificare la mancanza di una decisione totalmente automatica e, quindi, il suo momento, può risultare semplice in apparenza, in realtà è molto più complesso di quanto si pensi. Infatti, il variare del momento di concretizzazione del meccanismo di automazione del processo decisionale potrebbe influire, con un certo livello di incisività, sull'attivazione o meno delle tutele *ex* articolo 22. Inoltre, al variare del momento, potrebbe variare il soggetto che realizza l'automazione, in quanto la concatenazione delle parti coinvolte nel trattamento dei dati personali è spesso di complessa natura. Il *Working Party ex* Articolo 29 ha da tempo sostenuto, sempre nel parere WP251, che: "Il titolare del trattamento non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applicasse abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si avrebbe comunque una decisione basata unicamente sul trattamento automatico". Si asserisce così che il processo decisionale debba coinvolgere un essere umano a sua supervisione, il quale, se necessario, dovrebbe avere la possibilità di modificare la decisione presa, creando una correlazione di fatto. Secondo il gruppo, il coinvolgimento dovrebbe consistere in una serie di controlli (e di registrazioni da effettuarsi a mezzo DPIA) significativi e non fittizi, effettuati da una persona con l'autorità e la competenza necessari a modificare la decisione, prendendo in considerazione tutti i dati pertinenti[53].

Sul punto, la Corte di Giustizia europea (da qui anche CGUE), nella recente sentenza C-634/21[54], ha ampliato la fattispecie dell'articolo 22, come preliminarmente prospettato dal *Working Party ex* Articolo 29, allargandone il campo d'azione in termini di tempo e di soggetti.

Al fine di evidenziare il fulcro della decisione è necessario sintetizzare le relative vicende processuali. La causa nasce dalla richiesta della ricorrente di conoscere le dinamiche sottese al funzionamento di un *automatic decision making system* utilizzato ai fini di un diniego di una richiesta di credito. Il diniego della suddetta richiesta è avvenuto a seguito di informazioni elargite da un'agenzia di *credit scoring* ad un istituto di credito suo cliente. L'agenzia di *scoring* nell'assolvere alla richiesta

51. Malgieri–Comandé 2017.

52. Il parere WP251 è stato oggetto di ampio richiamo nel corso degli anni, risultando in più frangenti necessario ai fini di un'approfondita interpretazione dell'articolo 22. L'oggettiva difficoltà nel trattare una materia così complessa spiega perché, nonostante l'alta considerazione, il parere WP251 non sia esaustivo nell'interpretazione della norma e abbia ricevuto alcune critiche anche dalla dottrina. Per uno studio critico sul parere WP251 cfr. Veale–Edwards 2018.

53. Article 29 Data Protection Working Party 2017, p. 21.

54. Per un commento alla sentenza cfr. Horstmann 2024; Falletti 2024; Pietrella–Racioppi 2024.

di informazioni della ricorrente (ex articoli 13(2)(f), 14(2)(g) e 15(1)(h)[55]) ha precisato la propria estraneità alla decisione presa dall'istituto, allegando al contempo informazioni generiche circa le modalità di attribuzione del punteggio tramite software, rifiutandosi però di fornire dettagli sulle peculiarità algoritmiche del sistema, ritenendole protette dal segreto industriale. Dopo la ricezione delle suddette informazioni, la ricorrente presenta reclamo alla *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (HBDI), ossia l'Autorità Garante dello Stato dell'Hesse, ai fini di ingiungere l'agenzia ad accogliere la sua domanda di accesso alle informazioni[56]. La HBDI, con decisione del 3 giugno 2020, afferma di non ravvisare una violazione dell'articolo 31 della *Bundesdatenschutzgesetz* (BDSG)[57], la Legge Federale tedesca sul Trattamento dei dati personali del 30 giugno 2017, rigettando il reclamo della ricorrente[58]. Successivamente, la ricorrente, *ex* articolo 78 del GDPR, impugnando la decisione del Garante, ricorre al Tribunale Amministrativo di Wiesbaden (*Verwaltungsgericht Wiesbaden*)[59]. Secondo la Corte adita dalla ricorrente, il fulcro della contestazione è ravvisabile nell'individuazione del momento in cui la decisione automatica si è compiuta. Infatti, qualora l'automazione andasse a esaurirsi nella fase di valutazione da parte dell'istituto di credito che ha rigettato la richiesta sulla base dei dati forniti dall'agenzia, l'agenzia di *scoring* risponderebbe solo *ex* articolo 15(1)(h) ma non *ex* articolo 22(1), non potendo tra l'altro risponderne l'istituto di credito, in quanto non in possesso delle logiche utilizzate ai fini del calcolo di solvibilità[60].

Qualora invece la decisione venisse identificata con il calcolo di solvibilità compiuto dall'agenzia di *scoring*, questa risponderebbe degli obblighi di cui all'articolo 22(1). La Corte adita sottolinea come tale eventualità sfocerebbe in un possibile rapporto dicotomico tra l'articolo 22(1) del GDPR e l'articolo 31 della BDSG, introdotto ai sensi dell'articolo 22(2)(b)[61] del GDPR. Tale prospettiva sarebbe suffragata dal fatto che l'articolo 31 del BDSG considererebbe, nel trattamento dei dati, il solo uso dello *scoring* quale tecnica e non quale processo decisionale a sé stante, incidendo sul livello di tutela dell'interessato rispetto al divieto generale posto dall'articolo 22(1). Per cui, sempre secondo il Tribunale Amministrativo di Wiesbaden, l'articolo 31 della BDSG, considerando il solo uso dell'ADMS, potrebbe contrastare con il dettato dell'articolo 22(1), portando alla creazione di una lacuna nella tutela giuridica dell'interessato[62].

Dopo aver sospeso il procedimento, la Corte adita ha sottoposto alla CGUE la seguente questione pregiudiziale: "Se l'articolo 22, paragrafo 1, del [RGPD] debba essere interpretato nel senso che il calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito costituisce già una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici che riguardano l'interessato o che incide in modo analogo significativamente sulla sua persona, qualora tale tasso, calcolato sulla base di dati

55. Vedi punto 56, Corte di Giustizia europea (Sezione I), causa C-634/21, *OQ v. Land Hessen*.
56. Punto 17 causa C-634/21.
57. *Bundesdatenschutzgesetz*, Section 31: "For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if: 1. the provisions of data protection law have been followed; 2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure; 3. other data in addition to address data are used to calculated the probability value; and 4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented". Altresì consultabile nella traduzione italiana della Sentenza in causa C-634/21 al punto 13.
58. Punto 18, causa C-634/21.
59. Punto 19, causa C-634/21.
60. Punto 23, causa C-634/21. Così anche Falletti 2024, pp. 119-121.
61. Ovvero in ossequio a eventuali introduzioni normative da parte di uno Stato membro dell'Unione europea.
62. Punti 20-26, causa C-634/21.

personali relativi all'interessato, sia trasmesso dal titolare del trattamento a un terzo titolare del trattamento e quest'ultimo basi prevalentemente su tale tasso la sua decisione sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con l'interessato"[63].

La Corte di Giustizia europea, esprimendosi sulla prima questione pregiudiziale, ha sottolineato i caratteri principali dell'articolo 22(1), ribadendo come gli elementi cardine della norma, ossia la presenza di una decisione, la sua totale automazione, e la manifestazione di effetti significativamente incidenti sull'interessato, siano tutti cumulabili e necessari ai fini dell'applicazione delle tutele *ex* articolo 22; ravvisandone tutti gli elementi nel caso di specie.

Il *credit scoring*, secondo la Corte, rientrerebbe nell'ampia portata del combinato disposto dall'articolo 22(1) e del considerando 71 del GDPR. In assenza di una definizione normativa proposta dal Regolamento, la decisione di specie includerebbe una valutazione di vari aspetti dell'interessato e misure idonee a produrre effetti sullo stesso, ai quali dovrebbe avere il diritto di non essere sottoposto. L'ampia interpretazione della definizione di decisione rafforzerebbe di molto le tutele della norma, considerata sempre dalla Corte, per richiamo alle conclusioni dell'Avvocato Generale, quale divieto di principio[64] e non diritto esperibile all'occorrenza dall'interessato[65].

Sulla totale automazione, la Corte richiama il punto 33 delle conclusioni dell'Avvocato Generale[66], secondo il quale il *credit scoring* è pacificamente assimilabile a un sistema di profilazione,

63. Punto 27, causa C-634/21. Il Tribunale Amministrativo di Wiesbaden ha presentato anche una seconda questione pregiudiziale, ossia: "In caso di risposta negativa alla prima questione pregiudiziale: se l'articolo 6, paragrafo 1, e l'articolo 22 del [RGPD] debbano essere interpretati nel senso che ostano a una normativa nazionale ai sensi della quale il ricorso a un tasso di probabilità – nella fattispecie relativo alla solvibilità e alla disponibilità a pagare di una persona fisica, che includa informazioni sui crediti – di un certo comportamento futuro di una persona fisica, allo scopo di decidere sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con tale persona ("*scoring*"), è consentito solo se sono soddisfatte determinate ulteriori condizioni, meglio specificate nella motivazione della domanda di pronuncia pregiudiziale". Quesito cui la CGUE non ha risposto in quanto assolto attraverso la risposta alla prima questione pregiudiziale. Vedi punto 74, causa C-634/21.

64. Documento 62021CC0634, Conclusioni dell'avvocato generale P. Pikamäe, punto 31: "L'articolo 22, paragrafo 1, del RGPD presenta una peculiarità rispetto alle altre restrizioni al trattamento dei dati previste nel suddetto regolamento, nella misura in cui sancisce un 'diritto' dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione. Malgrado la terminologia impiegata, l'applicazione dell'articolo 22, paragrafo 1, del RGPD non richiede che l'interessato invochi attivamente il diritto. Infatti, un'interpretazione compiuta alla luce del considerando 71 di detto regolamento e che tenga conto dell'economia della disposizione di cui trattasi, in particolare del suo paragrafo 2, che enuncia i casi in cui un siffatto trattamento è eccezionalmente ammesso, consente piuttosto di concludere che la disposizione de qua prevede un *divieto generale* delle decisioni della tipologia sopra descritta. Ciò detto, va osservato che tale divieto si applica solo in presenza di circostanze molto specifiche, vale a dire, in concreto, alle decisioni 'che produc[ono] effetti giuridici che (...) riguardano [l'interessato] o che incid[ono] in modo analogo significativamente sulla sua persona'".

65. Punti 52 e 60, Case C634/21.

66. Documento 62021CC0634, Conclusioni dell'avvocato generale P. Pikamäe: "La disposizione in parola richiede, anzitutto, che esista un trattamento automatizzato di dati personali, fermo restando che, a giudicare dalla sua formulazione, la 'profilazione' è considerata una sua sottocategoria. A tal proposito, va osservato che lo scoring compiuto dalla SCHUFA ricade nella definizione legale contenuta nell'articolo 4, punto 4, del RGPD, posto che detta procedura utilizza dati personali per valutare determinati aspetti relativi alle persone fisiche per analizzare o prevedere aspetti riguardanti la situazione economica, l'affidabilità e il probabile comportamento di dette persone. Infatti, dal fascicolo della causa emerge che il metodo utilizzato dalla SCHUFA fornisce un 'punteggio di scoring' sulla base di determinati criteri, vale a dire, un risultato che consente di trarre delle conclusioni sulla solvibilità dell'interessato. Desidero, infine, sottolineare che nessuna delle parti coinvolte contesta la qualificazione della procedura di cui trattasi come 'profilazione', cosicché tale condizione può considerarsi soddisfatta nel caso di specie".

quest'ultima definita come sub-categoria rispetto all'insieme dei processi decisionali automatizzati[67].

Infine, sugli effetti giuridici e analoghi, la Corte conferma l'importanza del calcolo di solvibilità nel caso di specie (come nella quasi totalità dei casi simili[68]) quale elemento fondamentale ai fini del diniego di un prestito, da cui scaturiscono gli effetti significativi descritti dall'articolo 22(1) e dal considerando 71.

Per cui, ravvisati gli elementi essenziali dell'articolo 22(1) nel caso di studio, la CGUE ha asserito come il calcolo di solvibilità, considerata la *ratio* dell'articolo 22(1) e considerati gli obiettivi e le finalità perseguiti dal GDPR[69], sia dirimente rispetto alla concessione del prestito e, quindi, considerabile quale decisione automatizzata, anche se compiuta da un soggetto terzo, dal momento in cui l'istituto di credito, da cui dipende la stipula, vi attinge con forza nel prendere la decisione[70]. In altri termini, la Corte di Giustizia europea ha superato l'impostazione della Corte tedesca che aveva considerato lo *scoring*, effettuato da società come la SCHUFA, alla stregua di un mero atto preparatorio rispetto alla decisione assunta dal soggetto terzo di concedere o meno un prestito. Tale approccio restrittivo avrebbe comportato l'impossibilità per l'interessato di esercitare in modo effettivo il proprio diritto di accesso, poiché l'istituto, non avendo svolto direttamente l'attività di *credit scoring*, non avrebbe avuto a sua disposizione le informazioni richieste sul funzionamento dell'algoritmo utilizzato.

Nel complesso, la Corte ha collocato, in approccio sistemico e teleologico, le attività di *credit scoring* nel perimetro applicativo dell'articolo 22(1) e del considerando 71 del GDPR, evidenziando come, pur in assenza di una definizione normativa esplicita nel Regolamento, tale attività comporti una valutazione sistematica di molteplici aspetti personali dell'interessato, producendo effetti potenzialmente pregiudizievoli sulla sua sfera giuridica. Questa interpretazione estensiva della nozione di decisione rappresenta un punto di svolta significativo, poiché amplia considerevolmente l'ambito di protezione offerto dal Regolamento, ricomprendendo anche quelle valutazioni automatizzate che, pur non costituendo formalmente l'atto decisorio finale, ne determinano sostanzialmente il contenuto. La qualificazione operata dalla Corte trasforma profondamente la natura giuridica della disposizione in quanto l'articolo 22(1) del GDPR, malgrado la terminologia formalmente impiegata di "diritto", deve essere interpretato come espressione di un vero e proprio divieto generale a sottoporre l'interessato a decisioni interamente automatizzate. Tale ricostruzione, che la Corte fa propria nei punti 52 e 60 della sentenza, comporta conseguenze operative di primo piano, precedentemente ricostruite[71], imponendo al titolare del trattamento un obbligo preventivo di astensione.

La questione degli effetti giuridici e degli effetti analoghi significativi viene affrontata dalla Corte con un approccio sostanzialistico che valorizza l'impatto concreto sulla vita dell'interessato. Il calcolo di solvibilità rappresenta, come accennato, un elemento determinante ai fini della concessione o del diniego di prestiti, circostanza che produce effetti rilevanti sulla sfera giuridica ed economica dell'individuo, rendendo di fatto il processo decisionale automatizzato potenzialmente discriminatorio[72]. Tale considerazione è conseguenza della percezione espressa soventemente dagli intermediari di settore, secondo i quali all'uso di dati non tradizionali e di software maggiormente opachi non si accompagnerebbero rischi effettivi di manifestazione di meccanismi discriminatori verso la clientela[73].

67. Di portata più ampia, v. *supra* par. 3.
68. Punto 48, causa C-634/21.
69. Altrettanto importante ai fini della decisione è quanto sintetizzato dalla CGUE nei punti 41 e 51 della sentenza, ossia la contestualizzazione delle norme comunitarie rispetto alle circostanze di applicazione, da affiancare all'interpretazione letteraria e teleologica. Tale forma di interpretazione è spesso rimarcata dalla Corte per approccio cumulativo, sul punto v. Beck 2013, pp. 280-291 e giurisprudenza ivi citata.
70. Punto 73, causa C-634/21.
71. *Supra* par. 2.
72. Sulle discriminazioni algoritmiche cfr. Adinolfi 2022.
73. Pietrella–Racioppi 2024 le quali richiamano a Bonaccorsi di Patti–Calabresi–De Varti et al. 2022.

Per cui, è ravvisabile come le implicazioni della sentenza SCHUFA si estendano ben oltre il settore creditizio, prefigurando un modello regolatorio che si porrebbe in continuità con recente giurisprudenza comunitaria[74] e con il regolamento UE 2024/1689, c.d. AI Act, sull'intelligenza artificiale, il quale classifica i sistemi di valutazione del merito creditizio come ad alto rischio[75], imponendo requisiti stringenti di trasparenza, supervisione umana e non-discriminazione, in linea con l'interpretazione estensiva offerta dalla Corte.

È comunque da osservare come il suddetto allargamento operato dalla Corte potrebbe essere considerato alla stregua di una soluzione temporanea di stampo analogico, effettuata su un elemento normativo in sé già di difficile interpretazione letterale e sistemica, al fine di colmare una lacuna ricollegabile al complesso intreccio della catena del valore relativa all' intelligenza artificiale e alla tutela dei dati personali; probabilmente arginabile, allo stato attuale, solo tramite DPIA.

6. Conclusioni

L'analisi condotta sull'articolo 22 del GDPR conferma la cruciale rilevanza dell'articolo nel bilanciare innovazione tecnologica e protezione dei dati personali. È emerso come la qualificazione della norma quale divieto generale, temperato dalle eccezioni poste dal paragrafo 2 e integrato dal principio di *accountability*, costituisca l'interpretazione maggiormente aderente alla *ratio* del Regolamento. La peculiare costruzione degli elementi costitutivi della fattispecie, in virtù della complessa natura dei processi decisionali automatizzati, rivela come sia presente la necessità di un approccio ermeneutico sostanziale, orientato allo scopo, e non meramente formale, ai fini dell'efficace tutela dell'interessato.

Infatti, l'automazione è sempre stata oggetto di attenzione quando riferita ai dati personali. Non è un caso che la Direttiva 95/46/CE, punta di lancia europea sul tema per quasi venti anni, nacque con l'intento di ricomprendere nelle sue tutele i grandi sistemi di archiviazione e i dilaganti sistemi di automazione dei dati personali[76], di crescente utilizzo negli anni Novanta e ritenuti utili ai fini dello scambio di informazioni e allo sviluppo dell'Area Schengen[77]. Il risultato fu un importante balzo in avanti da un punto di vista normativo per tutti quei paesi, tra i quali l'Italia, dove la privacy, intesa come riservatezza, era nelle sue prime fasi di esplicita affermazione[78].

74. Recente giurisprudenza comunitaria, Corte di Giust. UE del 4 ottobre 2024, causa C-21/23, ha di fatto ampliato la portata applicativa del GDPR, ricomprendendovi fattispecie che in apparenza non vi rientrerebbero, il tutto al fine di fronteggiare, con maggior enfasi, i rischi scaturenti dall'attuale realtà digitale. In particolare, la sentenza ha assimilato alla categoria dei dati relativi alla salute, *ex* articolo 9 del GDPR, le informazioni necessarie a finalizzare una consegna a domicilio di medicinali.

75. Regolamento UE 2024/1689, allegato III.

76. Considerando 15 della Direttiva 95/46/CE: "considerando che il trattamento dei suddetti dati rientra nella presente direttiva soltanto se è automatizzato o se riguarda dati contenuti, o destinati ad essere contenuti, in un archivio strutturato secondo criteri specifici relativi alle persone, in modo da consentire un facile accesso ai dati personali di cui trattasi".

77. Russo–Scavizzi 2010 , p.42 e ss.

78. Il diritto alla riservatezza può essere inteso quale tutela di situazioni, o vicende, strettamente personali e familiari, dalle ingerenze di terzi sprovvisti di un interesse socialmente apprezzabile, indipendentemente se siano commesse o meno con mezzi leciti. Tale massima, rintracciabile in Cass. 27 maggio 1975, n. 2129, inerente alle controversie tra l'ex imperatrice Soraya Esfandiary e alcuni giornali, pone la definizione di un diritto, fino a quel momento, non riconosciuto esplicitamente da un punto di vista normativo. Si delinea così la riservatezza quale *ius excludendi alios*, marcandone l'elemento negativo, ovvero l'esclusione di altri soggetti dalla sfera privata. La mancanza di una esplicita menzione normativa del diritto alla riservatezza è sempre stata oggetto di studi da parte della dottrina, individuandolo quale implicita conseguenza della clausola generale di cui all'art. 2 della Costituzione. In tal senso: Auletta 1978, pp. 42 e ss. Inoltre, è stata oggetto di attenta analisi la mutevolezza e il rapporto di contiguità della riservatezza con altri diritti, oggetto di un'opera di bilanciamento continuo, come ad esempio in Busia 2000 il quale richiama De Cupis 1982, Gambaro 1981, Cerri 1991. Successivamente,

Il GDPR riprende l'impostazione umano-centrica della Direttiva 95/46[79], riproponendo la protezione dei dati personali attraverso un approccio improntato alla governance collaborativa, fondata sull'*accountability* dei titolari del trattamento, i quali, coscienti del sostrato normativo, pongono mezzi e modi idonei a garantire la circolazione delle informazioni, tutelando al contempo l'utenza.

Tale precisazione è importante se relazionata al tema trattato. Il GDPR nella sua effettiva applicazione, in forza dei principi introdotti, è malleabile rispetto alle innumerabili tipologie di trattamento dei dati personali, risultando applicabile a diversi settori tecnologici non ancora esistenti nelle fasi preliminari di costruzione del Regolamento.

Sul punto e con riguardo all'intelligenza artificiale, l'articolo 22 è considerabile quale architrave delle future tutele da uso improprio di informazioni. Pur nella sua vaga formulazione l'articolo 22, quando affiancato all'*accountability* del titolare, riesce a tutelare gli interessati dalle fattispecie di trattamento non espressamente tipizzate dal Regolamento[80]. La mancanza di una possibile identificazione di tutte le ipotesi di trattamento automatizzato, unitamente alla frammentarietà dei diversi ordinamenti giuridici che caratterizzano gli Stati membri dell'Unione europea, non rende agevole la regolamentazione di strumenti con cui il diritto stesso non riesce a stare al passo. Ne consegue un ampio uso di strumenti normativi orizzontali di diritto derivato, come lo sono i regolamenti comunitari, i quali, seppur idonei a deframmentare e dar veste alle diverse facce del digitale, rischiano di generare, come sapientemente illustrato in dottrina, disordine nell'ordine[81], attraverso il c.d. rischio di sovra regolamentazione.

La volontà di creare un'AI eticamente "buona" ma al contempo tecnologicamente e commercialmente valida crea non pochi interrogativi in punta di diritto. I quattro princìpi etici su cui un'AI dovrebbe essere costruita – equità, spiegabilità, rispetto dell'autonomia umana e prevenzione del danno[82] – sono noti da tempo, riversandosi totalmente nel testo dell'articolo 22, come palesato dalle vicende collegate a SCHUFA. Si può osservare come l'articolo 22 del GDPR rappresenti il sunto delle principali criticità collegate al diritto applicato alla tecnologia. La presenza di differenti contesti di trattamento non accorpabili in un singolo insieme, la presenza o meno di norme specifiche nei diversi ordinamenti europei[83], la "opacità" del dettato normativo, la sua contraddittorietà e il bilanciamento tra trasparenza e segreti industriali, sono solo alcune delle criticità emergenti dal paragrafo 1 dell'articolo 22 (a cui spesso deve fare fronte il fondamentale contributo di dottrina, autorità di controllo e giurisprudenza). Ed è qui che il bilanciamento giuridico tra etica ed economia deve necessariamente fare spazio a un terzo aspetto, teorizzato in essenziale letteratura scientifica decenni addietro[84], ovvero l'artificialità, da intendersi anche come l'attenzione normativa allo sviluppo contiguo e ineluttabile della tecnologia nella società contemporanea.

Per cui, a parere personale dello scrivente, l'approccio collaborativo orientato all'*accountability,* affiancato all'apposizione di un divieto di carattere generale, appare adeguato alla regolazione del

grazie alla spinta della DPD, nasce il Codice Privacy, D.lgs. 196 del 2003, corpo normativo dedicato alla tutela dei dati personali.

79. Considerando 2 della Direttiva 95/46/CE: "considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui".

80. È altresì osservabile come le qualità elastiche dei richiamati strumenti di governance collaborativa possano trasformarsi in autonome voci di rischio per entità, ad esempio societarie, medio-piccole. Infatti, la complessità e la genericità di alcune norme di settore potrebbero rendere difficoltose le operazioni di *compliance* per realtà dotate di strumenti economico-organizzativi limitati. Sul punto v. Schneider 2022, pp. 317-321.

81. Frosini 2023, pp. 37-38.

82. Sartor 2022, pp. 85-87.

83. Per una precisa ricostruzione in dottrina v. Malgieri 2019.

84. Con particolare riferimento a Frosini 1968.

fenomeno dei processi decisionali automatizzati, con buone prospettive di futuribilità. Tale considerazione nasce dal presupposto che l'approccio *by design* verso gli *automatic decision making systems* possa consentire, in futuro, una riduzione delle possibili inefficienze del divieto *ex* articolo 22, in quanto mitigabili, *ab origine*, da una ben ponderata gestione del rischio che tenga conto delle modalità di ingresso delle informazioni, prescindendo, in termini di modo, dalla tecnologia e dalle modalità di addestramento utilizzate. Infatti, la considerazione dell'articolo 22 quale solitario strumento di tutela, avulso dall'intero GDPR, porterebbe a un declino del divieto posto dall'articolo stesso. L'estensibile interpretazione degli elementi proposti dal paragrafo 1 dell'articolo 22, generici e non facilmente delineabili, potrebbe curiosamente garantire, in eccesso, l'ampia portata delle tutele fin qui descritte, divenendo però dipendenti dall'apporto di entità diverse dal legislatore, svalutando di conseguenza l'elemento letterale e definitorio (particolarmente apprezzabile nel diritto derivato) in favore di una frastagliata opera di interpretazione, rendendo nel tempo la norma inerte.

Quanto sopra esposto potrebbe trovare riscontro in un interessante studio[85]. Nella concreta applicazione delle disposizioni di *data protection* l'utente comune si ritrova, nella maggior parte dei casi, in una condizione di fraintendimento rispetto alle tutele che gli sono concesse, portando ad una erronea percezione delle stesse[86], rendendo il divieto di carattere generale preferibile rispetto al diritto di opposizione.

Nel concludere questa breve analisi sull'articolo 22(1) del GDPR, si può ribadire come la norma presenti senz'altro diversi problemi di interpretazione, ma la *ratio* generale dell'articolo sembra essere corretta e futuribile. La considerazione dell'articolo 22 quale divieto di carattere generale è idonea alla tutela dell'interessato e le deroghe concesse dal secondo paragrafo dell'articolo 22 lasciano ampi margini di manovra ai titolari, i quali possono attingere, nelle loro operazioni, a due ampie basi giuridiche di trattamento.

Riferimenti bibliografici

Aa. V.v. (2022), *L'intelligenza non è artificiale*, "Limes", 2022, n. 12

Article 29 Data Protection Working Party (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01)*, 2017

A. Adinolfi (2022), *Processi decisionali automatizzati e diritto antidiscriminatorio dell'Unione Europea*, in A. Adinolfi, A. Simoncini (a cura di), "Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche", Edizioni Scientifiche Italiane, 2022

T.A. Auletta (1978), *Riservatezza e tutela della personalità*, Giuffrè, 1978

E. Bayamlioğlu (2023), *Machine Learning and the Relevance of IP Rights: An Account of Transparency Requirements for AI*, in "European Review of Private Law", vol. 31, 2023, n. 2/3

G. Beck (2013), *The Legal Reasoning of the Court of Justice of the EU*, Bloomsbury Publishing, 2013

J. Bing (1981), *Information Law?*, in "Journal of Media Law and Practice", vol. 2, 1981, n. 3

E. Bonaccorsi di Patti, F. Calabresi, B. De Varti et al. (2022), *Intelligenza artificiale nel* credit scoring. *Analisi di alcune esperienze nel sistema finanziario italiano*, in "Questioni di Economia e Finanza", Occasional Papers, 2022, n. 721

R. Borruso (1997), voce *Informatica giuridica*, in "Enciclopedia del Diritto", Giuffrè, 1997

85. Gatt–Caggiano–Montanari 2021.

86. Vestoso 2021.

M. Brkan (2019), *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, in "International Journal of Law and Information Technology", vol. 27, 2019, n. 2

G. Busia (2000), voce *Riservatezza (diritto alla)*, in "Digesto delle Discipline Pubblicistiche", UTET, 2000

L.A. Bygrave (2020), *Article 22 Automated individual decision-making, including profiling*, in C. Kuner, L.A. Bygrave, C. Docksey (eds.), "The EU General Data Protection Regulation (GDPR). A Commentary", Oxford University Press, 2020

L.A. Bygrave (2019), *Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making*, in K. Yeung, M. Lodge (eds.), "Algorithmic Regulation", Oxford University Press, 2019

A. Caia, F. Iraci Gambazza (2022), *Articolo 22*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "GDPR e Normativa Privacy, Commentario", Wolters Kluwer, 2022

S. Calzolaio (2017), voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", UTET, 2017

A. Cavoukian, S. Taylor, M.E. Abrams (2010), Privacy by Design*: essential for organizational accountability and strong business practices*, in "Identity in the Information Society", vol. 3, 2010, n. 2

A. Cerri (1991), voce *Riservatezza (diritto alla)*, II - Diritto comparato e straniero, in "Enciclopedia Giuridica", vol. XXVII, Istituto dell'Enciclopedia Giuridica, 1991

R. Csernatoni (2024), *Charting the Geopolitics and European Governance of Artificial Intelligence*, Carnegie Europe, 2024

A. De Cupis (1982), *I diritti della personalità*, vol. IV del "Trattato di diritto civile e commerciale A. Cicu e F. Messineo", Giuffrè, 1982

A. Gambaro (1981), *Falsa luce agli occhi del pubblico/False Light in the Public Eyes*, in "Rivista di diritto civile", 1981, n. 1

G. D'Aquisto–M. Naldi (2017), *Big Data e privacy by design. Anomizzazione, Pseudonimizzazione, Sicurezza*. Giappichelli, 2017

G. D'Acquisto, C.A. Trovato, L. De Benedetti (2022), *Alcune riflessioni sul concetto di autonomia decisionale della macchina e sulle sue implicazioni regolamentari*, in A. Pajno, F. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione", vol. 1, il Mulino, 2022

L. Determann (2024), Determann's *Field Guide to Artificial Intelligence Law. International*, Edward Elgar Publishing, 2024

C. Di Francesco Maesa (2022), *La profilazione nel contesto del diritto internazionale*, in A. Adinolfi, A. Simoncini (a cura di), "Protezione dei dati personali e nuove tecnologie, Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche", Edizioni Scientifiche Italiane, 2022

E. Falletti (2024), *Alcune riflessioni sull'applicabilità dell'art. 22 GDPR in materia di* scoring *creditizio*, in "Il Diritto dell'informazione e dell'informatica", 2024, n. 1

T.E. Frosini (2023), *L'ordine giuridico del digitale*, in "Rivista interdisciplinare sul diritto delle amministrazioni pubbliche", 2023, n. 2

V. Frosini (1992), voce *Telematica e informatica giuridica - L'informazione automatizzata*, in Enciclopedia del Diritto, vol. XLIV, Giuffè, 1992

V. Frosini (1984), *Il diritto dell'informatica negli anni Ottanta*, in "Rivista trimestrale di diritto pubblico", 1984, n. 2

V. Frosini (1968), *Cibernetica diritto e società*, edizioni di comunità, 1968

L. Gatt, I.A. Caggiano, R. Montanari (eds.) (2021), *Privacy and Consent. A Legal and UX&HMI Approach for Data Protection*, Università degli Studi Suor Orsola Benincasa, 2021

M. Hildebrandt (2008), *Defining Profiling: A New Type of Knowledge?*, in M. Hildebrandt, S. Gutwirth (eds.), "Profiling the European Citizen", Springer, 2008

J. Horstmann (2024), *CJEU: The Rating of a Natural Person's Creditworthiness by a Credit Rating Agency Constitutes Profiling and Can Be an Automated Decision under Article 22w GDPR*, in "European Data Protection Law Review", vol. 10, 2024, n. 1

K.F. Hubert, K.N. Awa, D.L. Zabelina (2024), *The current state of artificial intelligence generative language models is more creative than humans on divergent thinking tasks*, in "Nature Scientific Reports", vol. 14, 2024

M.E. Kaminski (2019), *The Right to Explanation, Explained*, in "Berkeley Technology Law Journal", vol. 34, 2019, n. 1

M.E. Kaminski, G. Malgieri (2021), *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, in "International Data Privacy Law", vol. 11, 2021, n. 2

E.M. Le Fevre Cervini (2024), *Intelligenza artificiale: chi vuole restare indietro?*, ISPI, 9 maggio 2024

G. Malgieri (2019), *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in "Computer Law & Security Review", vol. 35, 2019, n. 5

G. Malgieri, G. Comandé (2017), *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in "International Data Privacy Law", vol. 7, 2017, n. 4

I. Mendoza, L.A. Bygrave (2017), *The Right Not to be Subject to Automated Decisions Based on Profiling*, in T.E. Synodinou, P. Jougleux, C. Markou, T. Prastitou (eds.), "EU Internet Law. Regulation and Enforcement", Springer, 2017

G. Pascuzzi (2016), *Il diritto dell'era digitale*, il Mulino, 2016

V. Pietrella, S. Racioppi (2024), *Il credit scoring e la protezione dei dati personali: Commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023*, in "Rivista italiana di informatica e diritto", 2024, n. 1

A. Pisapia (2018), *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, 2018

F. Pizzetti (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. 2, Giappichelli, 2016

R.J. Ricart, P. Álvarez-Aragonés (2023), *The geopolitics of Generative AI: international implications and the role of the European Union*, Real Instituto Elcano, 27 November 2023

V. Roppo (1984), *Un "diritto dei mezzi di comunicazione di massa"?* in "Rivista Critica del Diritto Privato", vol. 1, 1984

S. Ruggieri (2022), *Profile/Profiling*, in G. Comandé (a cura di), "Encyclopedia of Law and Data Science", Edward Elgar Publishing, 2022

S. Russo, R. Scavizzi (2010), *Manuale di diritto comunitario dell'informatica*, Giuffrè, 2010

C. Sarra (2020), *Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of* Contestability by Design, in "Global Jurist", vol. 20, 2020, n. 3

G. Sartor (2022), *L'intelligenza artificiale e il diritto*, Giappichelli, 2022

G. Sartor, F. Lagioia (2020), *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Study EPRS PE 641.530, June 2020

G. Schneider (2022), *Intelligenza artificiale,* governance *societaria e responsabilità sociale d'impresa: rischi e opportunità*, in A. Pajno, F. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione? Proprietà intellettuale, società e finanza", vol. 3, il Mulino, 2022

M. Taher Pilehvar, J. Camacho-Collados (2021), *Embeddings in Natural Language Processing. Theory and Advances in Vector Representations of Meaning*, Springer, 2021

L. Tosoni (2021), *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, in "International Data Privacy Law" vol. 11, 2021, n. 2

M. Veale, L. Edwards (2018), *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in "Computer Law & Security Review", vol. 34, 2018, n. 2

M. Vestoso (2021), *Clues of mismatch between legal and users' conception of personal data protection,* in L. Gatt, R. Montanari, I.A. Caggiano (eds.), "Privacy and Consent. A Legal and UX&HMI Approach for Data Protection", Università degli Studi Suor Orsola Benincasa, 2021

S. Wachter, B. Mittelstadt, L. Floridi (2017), *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in "International Data Privacy Law", vol. 7, 2017, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0152 • articolo sottoposto a peer review • pubblicato in anteprima il 18 giu. 2025
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Alfonso Contaldo

Cenni sulla funzionalità dell'atto amministrativo con l'ausilio dei Sistemi Esperti

Nonostante si parli sempre più spesso di amministrazione digitale, tuttavia non tutta l'attività della pubblica amministrazione può essere automatizzata con l'impiego dei Sistemi Esperti. Il software è dotato di una propria "logica" che governa il suo procedimento decisionale, secondo la quale un problema si può risolvere solo se riconducibile ad una sequenza di istruzioni che indicano in modo preciso i passi da compiere, partendo da certe informazioni: l'algoritmo, appunto, e la logica dei programmi condizionali if-then. Ciò significa che il precetto normativo deve poter essere suddiviso in due gruppi di parole: la protasi che delinea i presupposti affinché si verifichino determinate circostanze; l'apodosi in cui le conseguenze sono statuite. I limiti della c.d. formalizzazione del processo di ragionamento, ossia di quella procedura computazionale intellegibile dall'uomo quale è l'algoritmo, fanno sì che l'attività per la quale è possibile effettuare tale formalizzazione risulti essere in primis quella cd. vincolata, mentre quella discrezionale richiede una diversa attività di programmazione dell'algoritmo con più varianti, attivabili con i sistemi di IA. I Sistemi Esperti si presentano attualmente come una soluzione altamente proficua.

Automazione – Atto amministrativo – Formalizzazione – Sistemi Esperti

Notes about the functionality of the administrative act with the Expert Systems aid

Although digital administration is an increasingly common topic, not all public sector activities can be automated by Expert Systems. These systems operate according to an internal "logic" that governs their decision-making process: a problem can be solved only if it can be translated into a sequence of instructions that clearly define the steps to be followed, starting from specific input data. This is the essence of the algorithmic model and the logic of conditional if–then programming. Accordingly, a legal norm must be expressible as two distinct components: the *protasis*, which defines the necessary conditions for a given situation; and the *apodosis*, which determines the corresponding consequences. The limitations of the so-called formalization of reasoning processes – i.e., computational procedures intelligible to humans, such as algorithms – imply that only activities that can be fully formalized are suitable for automation. These are primarily the so-called constrained decisions, whereas discretionary decisions require a different approach to algorithm design, involving a broader range of variables. In this context, Expert Systems emerge as a particularly promising solution for the effective use of artificial intelligence.

Automation – Administrative act – Formalization – Expert Systems

L'Autore è dottore di ricerca in Informatica giuridica e diritto dell'informatica presso Sapienza - Università di Roma, docente di Diritto dell'informazione e della comunicazione digitale nell'Accademia delle Belle Arti di Roma, docente a c. di Informatica giuridica nell'Università di Roma Tre

Sommario: 1. Premesse. – 2. Il software e la decisione dell'atto amministrativo. – 3. La previsione dell'atto-software ed il Sistema Esperto. – 4. I limiti all'automazione delle decisioni amministrative a carattere discrezionale dell'attività amministrativa. – 5. Sistemi Esperti: un'applicazione consolidata per le attività amministrative non discrezionali.

1. Premesse

Il diritto, come la totalità dei vari ambiti del vivere associato, è profondamente ed inevitabilmente mutato con il progresso delle ICT e l'avvento dell'IA; perfino il lavoro del funzionario pubblico può essere in parte automatizzato, come del resto già sviluppato con l'impiego dei Sistemi Esperti Legali[1] anche nell'amministrazione pubblica italiana.

Si vuole così sottolineare che la maggioranza dell'attività della P.A., considerata nel suo complesso e nelle sue ramificazioni, può essere ad oggi svolta con le ICT[2]; anzi, che il *modus operandi* dell'amministrazione dovrebbe essere improntato sulla modalità ICT, che è in grado di dar seguito ai principi di efficienza, economicità, efficacia, trasparenza, buon andamento ed imparzialità enucleati all'art. 97 Cost.[3]

1. I sistemi esperti rappresentano attualmente un'applicazione conosciuta e consolidata nell'impiego dell'informatica nel diritto; può dimostrarsi infatti, che esiste un'adeguata corrispondenza tra le loro possibilità applicative e le caratteristiche fondamentali del ragionamento giuridico orientato alla risoluzione di problemi e alla formulazione di decisioni. La rapida evoluzione delle tecnologie informatiche, i continui progressi ottenuti nella realizzazione di software di alto livello e, in generale, il clima di grande interesse e alta competitività che si è creato in questi ultimi anni intorno alle potenzialità e agli sviluppi della ricerca nel campo dell'Intelligenza Artificiale hanno reso disponibile una notevole quantità di strumenti di supporto alla realizzazione di sistemi esperti, che spaziano in una gamma ampiamente articolata, dai linguaggi di programmazione generali a prodotti applicativi finiti (chiavi in mano). In quest'ambito, gli shells in particolare sembrano destinati ad assumere un crescente interesse per il giurista che voglia cimentarsi personalmente nella realizzazione di sistemi atti a supportare la sua attività. Oggetto dell'analisi diventano allora l'individuazione dei requisiti che i sistemi esperti dovrebbero possedere per essere considerati validi supporti tecnici nei confronti della decisione dell'operatore giuridico e, in corrispondenza, la selezione degli strumenti che sarebbe più opportuno utilizzare per la realizzazione di tali sistemi. La valutazione degli strumenti e delle metodologie per la costruzione di sistemi esperti in campo giuridico però non può essere condotta astrattamente sulla base di schemi concettuali rigidi, ma deve tener conto della varietà dei problemi e della molteplicità degli aspetti che il diritto presenta. Vedi Caridi-Pellecchia 1986, p. 72; i saggi in Mariani-Tiscornia 1989; Lucatuorto 2006, p. 219 ss.; Lucatuorto 2009, p. 82 ss.; vedi anche Contaldo-Campara 2020, p. 45 ss.
2. Vedi Frosini 1983, p. 48 ss., che già preconizzava questa possibilità.
3. Vedi Allegretti 1965; Allegretti 1993, p. 864 ss.; Allegretti 1998, p. 92 ss.; Allena 2012, p. 569; Amirante 2004, p. 171; Barile 1958; Carlassare 1974; Cassese 1973; Cassese 2007, p. 13; Cassese 2011, p. 105; Cerri 1973; Cerri 1992, p. 1526; Cerri 1998; Cerri 2006; Cerri 2009; Cerbo 2007; Cerri-Galeotti 2012; Chirichiello 2000; D'Auria 2009, p. 3079; Ferrara 2011, p. 335.

L'atto amministrativo prodotto da ICT non scaturisce dalla "volontà" di un elaboratore elettronico, ma è, al pari di ogni altro atto amministrativo analogico, il frutto di un procedimento[4], ovvero di un insieme di atti teleologicamente collegati (c.d. infraprocedimentali) che conducono all'emanazione di un provvedimento, il quale sintetizza e riassume in sé tutti gli atti del procedimento. Affinché ciò sia possibile è necessario che il computer sia istruito da un Sistema Esperto, ovvero sia in grado di generare un'operazione complessa caratterizzata da un insieme di atti teleologicamente orientati al risultato.

L'automazione della P.A. può toccare numerosi profili e momenti sia nell'ambito dell'organizzazione che dell'attività. Sebbene alla formula "sistemi informativi automatizzati"[5] sia possibile attribuire in astratto una moltitudine di significati, nei contesti in cui è stata impiegata indica genericamente la gestione dei dati, ossia la loro reperibilità mediante opportuni software di ricerca su banche dati strutturate *ad hoc*.

Gli atti amministrativi automatizzati non ineriscono esclusivamente l'amministrazione digitale, ma anche quella attuale, non del tutto digitalizzata nonostante le ripetute previsioni normative, come da ultimo le previsioni di cui al d.l. n.162 del 2019, convertito in legge n. 8 del 2020. La differenza macroscopica tra le due versioni di P.A. risiede nella modalità di impiego del computer e del Sistema esperto: da un lato si ha un'amministrazione comunque non ancora digitale, in cui il computer predispone l'atto automatizzato che in un secondo momento potrà essere stampato; in questo caso non vengono sfruttate a pieno le potenzialità offerte dal computer e dunque minori saranno i benefici ottenibili. Dall'altro vi è invece un'amministrazione che, conscia delle caratteristiche e dei vantaggi delle ICT, opera in un contesto informatizzato e digitalizzato in cui il computer, in senso lato, è il cuore pulsante dell'azione amministrativa[6]. In questa P.A. evoluta anche il procedimento amministrativo viene informatizzato, anche perché si presta a tale operazione. Il procedimento amministrativo è stato definito come "la serie concatenata di atti provenienti da soggetti pubblici (organi e uffici) e anche da soggetti privati […] e di operazioni […] preordinati alla produzione di un provvedimento finale, come tale suscettibile di produrre effetti innovativi nell'ordinamento"[7]. Il procedimento amministrativo si suddivide in varie fasi: quella del reperimento degli interessi coinvolti, quella della decisione, quella (eventuale) dell'integrativa dell'efficacia; fasi, queste, che normalmente vengono gestite dal personale amministrativo ed ora anche dei Sistemi Esperti, che provvedono alla soddisfazione di tutte le esigenze che si sviluppano nell'iter procedimentale[8].

2. Il software e la decisione dell'atto amministrativo

La automatizzazione del procedimento decisionale dell'atto amministrativo fa emergere naturalmente nuovi problemi rispetto alla tradizionale cultura giuridica dell'adozione dell'atto da parte del funzionario[9].

Nel linguaggio tecnico, il software è l'insieme delle istruzioni che l'elaboratore utilizza per ottenere da certi dati in ingresso (input) un certo risultato di uscita (output)[10].

"Istruire" in linguaggio informatico indica non il processo di apprendimento delle nozioni necessarie allo svolgimento di una data attività, bensì la codifica di un ordine eseguibile.

4. Vedi Bartolini-Fantini-Ferrari 2010; Caranta 2008; Caringella-Protto 2009; Cognetti 2010; Comporti 2001; Della Cananea 2008; Della Cananea 2007; Falcon 2008; Figorilli 1996; Garofoli 2009; Lazzara 2008; Marenghi 2009; Massera 2008; Mattarella 2009, p. 247; Arena-Corso-Gardini et al. 2008; Merusi 2009; Morbidelli 2005, p. 635 ss.; Occhiena 2002; Sandulli 2011.
5. Ancora Frosini 1983.
6. Vedi Carloni 2014; Costantino 2012; De Minico 2011; Gallone 2023, p. 84 ss.; Masucci 2011; Masucci 2000; Mattarella 2005; Arena-Corso-Gardini et al. 2008; Marongiu 2005, p. 74 ss.
7. Così Morbidelli 1998, p. 997.
8. Vedi Contaldo-Gorga 2006, p. 177; Notarmuzi 2008, p. 366 ss.
9. Vedi Masucci 2011, p. 82 ss.
10. Cfr. Usai 1993, p. 173.

Per istruire il programma è necessario, *in primis*, procedere con la formalizzazione dei dati di fatto o di diritto. Si tratta di un momento in cui i principi giuridici generali, le proposizioni normative e le massime giurisprudenziali pertinenti al problema, vengono tradotti in linguaggio formale; in più, tramite la formalizzazione si converte in linguaggio formale anche l'elemento fattuale, ovvero l'avvenimento della vita che, trovando la sua corrispondenza in una norma di diritto, produce determinate conseguenze[11]. Altrimenti detto, si tratta di fornire al calcolatore delle regole logico-matematiche codificate in un linguaggio tecnico e tratte da percorsi di razionalizzazione dell'attività umana[12]. Tali regole devono essere precise, inequivoche, generali ed astratte, formulate *ex ante* e tese ad un risultato, di primo grado a carattere tecnico.

Il passo successivo è rappresentato dalla c.d. formalizzazione del processo di ragionamento. La stesura di queste istruzioni richiede la scomposizione del problema in una successione di sotto-problemi elementari, risolvibili in base ad una regola nota[13]. In altri termini, per far sì che il Sistema Esperto possa risolvere un problema, bisogna che questo sia traducibile in un algoritmo, ossia in un numero finito di passaggi che, partendo dai dati a disposizione e seguendo lo schema logico dell'if-then (se-allora), conduca alla soluzione del problema.

La definizione, *rectius* pre-determinazione, dell'atto-programma è un momento cruciale per l'*agere administrandi* poiché è in questa sede che si perviene ad una sintesi della valutazione delle situazioni fondamentali per l'esercizio di uno specifico potere amministrativo[14]. Questa sintesi si effettua in base allo schema dei c.d. programmi condizionali (l'if-then appunto), per cui ogni volta che si realizza la fattispecie concreta (A) segue la decisione (B).

L'algoritmo dunque presenta tre tratti essenziali: risolve sempre il problema, in maniera univoca e in un numero finito di passaggi. Con l'atto-software la P.A. può collegare ogni possibile fattispecie futura, allo stato ipotizzabile, ad un insieme determinato e finito di contenuti del provvedimento e questo grazie ad una preventiva selezione tra gli elementi fattuali rilevanti per l'esercizio del potere e ad una valutazione altrettanto anticipata degli interessi.

L'elaboratore trasforma dei dati quantificabili (input) in dati in uscita (output) senza svolgere alcun ragionamento autonomo, per così dire, ma applicando istruzioni dapprima strutturare in un algoritmo (procedura computazionale intellegibile dall'uomo) e successivamente tradotte in un software (procedura computazionale intellegibile della macchina)[15], mentre il Sistema Esperto procede a risolvere autonomamente problemi giuridici anche complessi sulla scorta di procedure di inferenze adeguate (logico-computazionali). Un sistema esperto è infatti un software che, dopo essere stato adeguatamente istruito, è capace di dedurre informazioni (output) da un insieme di dati e da informazioni di partenza (input).

Si potrà dunque avere una decisione automatizzabile se la disposizione normativa potrà essere codificata in modo chiaro ed univoco, come vuole la logica binaria tipica delle macchine, cosicché si fornisce l'istruzione idonea a determinare il contenuto dell'atto; se, dunque, sarà possibile individuare una serie finita di passaggi logici, legati dal nesso di consequenzialità, in virtù dei quali, a partire da un certo problema, si potrà giungere ad un risultato univoco, secondo uno schema sillogistico.

Quindi se in una procedura amministrativa o nell'emanazione di un provvedimento interviene un elaboratore elettronico non solo in qualità di fornitore di dati ma anche come esecutore di operazioni logiche, è chiaro che il giurista focalizzerà la propria attenzione sull'esame della fase della programmazione della macchina, del computer[16].

Ci si interroga dunque sulle possibilità che le ICT offrono se impiegate per codificare il processo decisionale finalizzato alla decisione amministrativa automatizzata o ad elaborazione elettronica,

11. Vedi Sartor 2022.
12. Vedi Duni 1978, p. 407 ss.
13. Vedi Fantigrossi 1992, p. 51; Usai 1993, p. 17 ss.
14. Vedi Natoli 2003, p. 958 ss.
15. Vedi Otranto 2018, p. 15.
16. Vedi Fantigrossi 1992, p. 51.

passando dal "computer archivio" al "computer funzionario"[17].

Tuttavia anche la formalizzazione non è immune da limiti o criticità di carattere logico e giuridico. Anzitutto la formalizzazione richiede come presupposto una corrispondenza univoca dei significanti ai loro significati, una sintassi regolare ed invariabile. Risulta quindi impossibile applicare al computer normative che contengono concetti giuridici indeterminati. La ragion d'essere della formalizzazione risiede nel depurare il testo di legge da ogni tipo di ambiguità sintattica attraverso una riformulazione che ne esprima la struttura logica in maniera univoca. Perciò il documento normativo viene scomposto in enunciati elementari, di forma sintatticamente compiuta e dotate di autonomia semantica. Ma il problema si pone nel momento in cui è il termine stesso a portare un'indeterminatezza semantica di concetti giuridici o fattuali, per i quali è invece possibile attribuire una molteplicità o variabilità di significati. È dunque impossibile predeterminare i significati riferibili al termine e procedere ad una sua formulazione in linguaggio standard. In questo caso allora ecco che torna in auge l'operato dell'interprete, il cui Sistema Esperto sarà quello di rintracciare il significato esatto da attribuire al termine e di affidare al computer, in un secondo momento, il prosieguo del procedimento attraverso una combinazione del momento informatico con quello manuale. In questo caso, al pari di altri che analizzeremo, la commistione dell'elemento virtuale-informatico con quello umano-manuale non si configura come un'inefficienza nell'impiego delle risorse od un'inefficacia dell'azione amministrativa, o ancora come una duplicazione del lavoro sia sul supporto cartaceo che su quello digitale, ma è anzi una delle possibili soluzioni a disposizione dell'amministrazione per articolare e gestire il proprio lavoro.

Un secondo ordine di limiti concerne l'algoritmo: precisamente, il nesso di derivazione tra il se-premessa maggiore e l'allora-premessa minore deve essere indubbio, chiaro, privo di contraddizioni logiche o di lacune, e scomponibile in una serie di enunciati elementari[18].

Un terzo limite, affrontato specificamente nel prosieguo della trattazione, attiene invece alla natura dell'attività da formalizzare, vale a dire se essa sia vincolata o discrezionale.

Se il software governa, per così dire, lo sviluppo del procedimento e contemporaneamente determina *ex ante* il contenuto del singolo atto in relazione allo specifico input, allora le istruzioni inserite nell'atto-programma devono rispettare principi e norme di carattere sostanziale e procedimentale relative alle fattispecie da regolare. In estrema sintesi, la legge governa la redazione del programma, mentre il programma governa il procedimento[19].

Il programma quindi altro non fa che tradurre la disciplina normativa del procedimento *de quo* in istruzioni (passaggio da una tipologia ad un'altra di linguaggio) e stabilire la "logica" del procedimento decisionale, cioè il *modus procedendi* dell'amministrazione.

3. La previsione dell'atto-software ed il Sistema Esperto

In tema di qualificazione giuridica dell'atto-software si registrano in dottrina essenzialmente due opposte visioni, tra chi riconosce all'atto-programma la natura di atto amministrativo, pur con differenze sostanziali, e chi non gli attribuisce tale natura.

Quasi unanimemente la dottrina tende a far risalire il fondamento giuridico dell'atto-programma ai principi di imparzialità e buon andamento ex art. 97, Cost., che devono sempre informare la potestà delle istituzioni pubbliche[20]. Ma è soprattutto al disposto dell'art. 12, l. n. 241/1990, secondo il quale sorge in capo alla medesima amministrazione l'obbligo di predefinire le regole della propria azione manifestate successivamente in modo da assicurare il sindacato giurisdizionale[21].

L'atto programma presenta una natura astratta, considerando che i destinatari del provvedimento automatizzato, singolarmente e normativamente

17. Così Otranto 2018, p. 15.
18. Vedi Contaldo-Gorga 2006, p. 194 ss.
19. Vedi Masucci 2011, p. 84.
20. Vedi per tutti Giannini 2000, p. 682 ss.
21. Cfr. Natoli 2003, p. 958; Masucci 2011, p. 86; Otranto 2018, p. 16.

intesi, non sono individuati *a priori*. Questo risulta essere in linea con il fatto che il provvedimento sia finalizzato alla risoluzione di ogni possibile caso e dunque è frutto pure della considerazione in concreto dei vari elementi soggettivi rilevanti per emanare l'atto. I soggetti, sebbene non siano individuabili in via preventiva, sono identificabili poiché ricompresi nei tipi considerati in fase di determinazione dei contenuti dell'atto. Questa identificazione avverrà in un momento successivo, precisamente in fase di esecuzione o applicazione dell'atto-software e poi in sede di emanazione dell'atto amministrativo informatico, ed è solo in questa occasione che si inseriranno i dati concernenti la singola fattispecie[22]. I dati, elaborati secondo quanto stabilito nell'atto-software, condurranno all'individuazione dell'atto puntuale che provocherà effetti nella sfera giuridica soggettiva del destinatario.

Quindi nulla osta a considerare l'atto-software alla stregua di un atto amministrativo secondo la definizione tradizionale, in quanto il contenuto dell'atto-programma presenta un oggetto "determinabile"[23].

Con l'emanazione dell'atto-programma si ha una differente articolazione del procedimento per l'adozione degli atti ad esso conseguenti. L'automazione comporta, allora, la scissione del procedimento in due momenti distinti: *in primis*, il procedimento che porta all'adozione dell'atto-software, all'interno del quale si collocheranno le fasi relative alla determinazione di tutti i possibili contenuti, al momento attuale, di futuri provvedimenti puntuali; *in secundis*, il procedimento per questi ultimi, in cui oltre all'iniziativa verranno inserite le attività degli interessati e dell'amministrazione per appurare la corrispondenza tra la singola situazione e quelle già considerate e previste in sede di programmazione.

Se la fattispecie astratta è costituita dal software, ossia da un elemento dato e relativamente immodificabile, l'input e l'atto amministrativo informatico rappresentano la fattispecie concreta che, secondo il procedimento di sussunzione, corrisponde proprio allo schema predeterminato dall'elaboratore. Con il termine input si intende il complesso delle informazioni che l'amministrazione è tenuta a raccogliere ed inserire nel computer nella fase di avvio del procedimento, corrispondente ad una vicenda della vita reale, identica a quella stigmatizzata dal programma. Per quanto riguarda la provenienza dei dati da acquisire, essi possono essere interni all'amministrazione stessa o esterni, cioè nel possesso o nella disponibilità di privati o di banche dati di altre amministrazioni, la cui acquisizione può avvenire mediante l'operato umano o anche un software del computer a ciò predisposto.

Ciò che segue l'immissione dell'input all'interno del programma dell'elaboratore è l'atto amministrativo informatico produttivo di effetti immediati nella sfera giuridica dei destinatari. Ed è proprio sulla natura giuridica di tale tipologia di atto che il dibattito dottrinale, non solo italiano, si è particolarmente sviluppato.

Per la dottrina dominante l'atto amministrativo informatico costituisce pienamente un atto amministrativo[24], dove per volontà si intende la volontà procedimentale e non quella civilistica, ovverosia l'imputabilità (intesa oggettivamente nel senso di riferibilità) del medesimo all'autorità amministrativa. Seguendo questo ragionamento si può configurare la c.d. volontà dell'elaboratore come volontà della p.a., una volontà circoscritta ma in armonia con i principi fondamentali dell'azione amministrativa. Non si ravvisa dunque alcuno scollamento tra la volontà dell'amministrazione e la volontà, per così dire, dell'atto che resta sempre espressione dell'autorità amministrativa.

Il Sistema Esperto, non essendo dotato di una propria capacità di intendere e di volere, è solamente l'estensione dell'amministrazione procedente e gli atti che da esso scaturiscono non si differenziano da quelli prodotti manualmente dai suoi funzionari e dai suoi uffici. Sostenere il contrario, e cioè che il Sistema Esperto possa avere non solo una volontà propria ma anche potenzialmente diversa da quella dell'amministrazione cui appartiene, sarebbe una contraddizione in termini visto che il software è strutturato in via preventiva in ogni sua componente proprio dalla P.A.[25]

22. Vedi ancora Natoli 2003.
23. Vedi Fantigrossi 1992, p. 110.
24. Vedi per tutti Masucci 2011.
25. Vedi *Ivi*, p. 224; Duni 2008, p. 76 ss.

L'amministrazione pubblica è e continua ad essere il *dominus* dell'intero procedimento, secondo l'equazione matematico-giuridica per cui il computer potrà dar seguito solo alle operazioni previste dal programma adottato dalla P.A. In base al principio *causa causae est causa causati*, la volontà del Sistema Esperto è geneticamente volontà dell'amministrazione che ha predisposto o deciso di impiegare uno specifico programma.

Nel momento in cui l'amministrazione decide di adottare un programma diventa conseguentemente responsabile del medesimo e dei singoli atti futuri che ne scaturiranno in esecuzione proprio del programma. L'elaboratore altro non è che uno strumento nella disponibilità dell'amministrazione per conseguire i propri obiettivi. Senza dimenticare che l'atto conclusivo del procedimento adottato mediante computer viene comunicato dall'amministrazione stessa, a suo nome, al destinatario e sempre a suo nome ne richiede l'osservanza. In caso contrario si rischierebbe di de-responsabilizzare l'amministrazione, con pregiudizio per i cittadini nel fare affidamento alla fede pubblica.

Al pari dell'atto amministrativo, dunque, anche l'atto amministrativo informatico presenta quali elementi essenziali il soggetto emanante, il destinatario, la forma, il contenuto, la finalità istituzionale (ossia la "causa procedimentale"), ed infine la motivazione.

4. I limiti all'automazione delle decisioni amministrative a carattere discrezionale dell'attività amministrativa

Tuttavia non tutta l'attività della P.A. può essere automatizzata. Il Sistema esperto è dotato di una propria "logica" che governa il suo procedimento decisionale, secondo la quale un problema si può risolvere solo se riconducibile ad una sequenza di istruzioni che indicano in modo preciso i passi da compiere, partendo da certe informazioni: l'algoritmo, appunto, e la logica dei programmi condizionali if-then. Ciò significa che il precetto normativo deve poter essere suddiviso in due gruppi di parole: la protasi che delinea i presupposti affinché si verifichino determinate circostanze; l'apodosi in cui le conseguenze sono statuite.

Abbiamo in precedenza accennato ai limiti della c.d. formalizzazione del processo di ragionamento, ossia di quella procedura computazionale intellegibile dall'uomo quale è l'algoritmo[26]: ci soffermiamo ora sulla natura dell'attività per la quale è possibile effettuare tale formalizzazione, che può essere di tipo vincolato oppure discrezionale.

Vincolatività e discrezionalità non sono categorie da intendere in modo rigido ed assoluto, ma al loro interno vengono riconosciute declinazioni e sfaccettature più che utili per il tema dell'automazione che stiamo indagando[27]. L'aggettivo "vincolato" viene attribuito ai quei procedimenti che necessitano solamente di una verifica circa il possesso di determinati requisiti richiesti dalla norma. Altro discorso è da fare, invece, per quanto riguarda i procedimenti "discrezionali", quelli per i quali occorre una valutazione degli interessi in gioco, siano essi pubblici o privati, individuali o collettivi. A differenza di quella discrezionale, l'attività vincolata, essendo compatibile con la logica del computer, non ha posto rilevanti problemi circa una sua possibile automatizzazione, tant'è che è in questo senso che si è espressa la stragrande maggioranza della dottrina[28]. Si fa risalire la necessità della vincolatività ai tratti caratteristici della programmazione del computer, la quale procede per step logici predeterminati, di modo che la determinazione da assumere in date circostanze sia univoca. Stando all'orientamento dominante, se una norma precisa stabilisce inequivocabilmente in quali circostanze la P.A. debba provvedere e se il contenuto dell'atto rende automatica l'emanazione dell'atto stesso, allora il compito in esame può essere affidato al calcolatore.

Dunque se un'attività o un settore di attività sono meramente esecutivi, cioè privi di alcun margine di discrezionalità e di apprezzamento da parte dell'amministrazione, possono essere completamente ed agevolmente soggetti all'automazione. L'assenza di discrezionalità amministrativa è il presupposto affinché si possa parlare di attività vincolata o, meglio, si possa avere lo schema if-then. A seguire si deve costruire la fattispecie

26. Vedi ancora Otranto 2018, p. 15.

27. Deodati 2017, p. 71 ss.

28. Duni 2008, p. 77; Masucci 2011, p. 125; Torchia 2023, p. 72 ss.

astratta attorno a concetti giuridici analitici (della matematica o, in generale, delle c.d. scienze esatte) capaci di quantificare la realtà, così da rendere il sistema automatizzato in grado di realizzare in modo uniforme, efficiente, versatile e veloce le attività che compirebbe un funzionario pubblico.

L'attività vincolata ben può essere svolta dalla macchina-computer in completa autonomia[29], sottraendo alla fase istruttoria ogni tipo di intervento umano, anche quando si debba accedere a banche dati presso altri enti, dal momento che, in un sistema in cui la cooperazione applicativa è garantita, saranno interoperabili; del resto, è stato sostenuto che il fondamento giuridico del potere di adottare un programma per l'automatizzazione dell'attività vincolata deriva dalla potestà organizzatoria tipica di ciascun ente[30]. C'è da dire che questa scelta organizzativa risulta in linea con il principio di ragionevolezza e di logicità, dal momento che l'automazione adduce indubbi benefici riguardanti la riduzione del rischio di disparità di trattamento, l'osservanza della legge, la prevenzione di fenomeni corruttivi, la completezza dell'istruttoria, divenendo uno strumento volto a realizzare l'imparzialità ed il buon andamento dell'amministrazione.

Un discorso diverso va invece affrontato per quanto riguarda la c.d. discrezionalità tecnica. L'attributo "discrezionale" associato a tale attività induce in errore nel considerarla un'attività discrezionale vera e propria[31], dal momento che non si opera un giusto contemperamento degli interessi. La discrezionalità tecnica si manifesta in occasione dell'emanazione di un atto per il quale è indispensabile valutare alla stregua di conoscenze tecniche come, ad esempio, quelle dell'arte, della fisica, della medicina. Qui si riconosce l'applicabilità dei medesimi criteri validi per la discrezionalità amministrativa, sebbene il caso *de quo* non rilevi per una scelta tra interessi, ma pur sempre riguardi una decisione tra opzioni diverse ed opinabile nel significato.

Se il Sistema Esperto abbisogna di termini certi ed inequivocabili affinché possa pervenire autonomamente ad una decisione finale, in questo caso non si potrà disporre di quella certezza, dato che l'individuazione del significato più giusto ed appropriato da attribuire al concetto in esame è delegata all'esperto.

A questo punto si ritiene che le fattispecie a bassa discrezionalità tecnica siano compatibili con la logica dell'elaboratore, poiché in questo caso gli atti sono sottoponibili ad autolimite da parte dell'amministrazione titolare del potere, qualora l'autolimite sia fissato in termini precisi e dunque traducibili in linguaggio computazionale[32]. Al contrario, le fattispecie ad alta discrezionalità tecnica risultano meno compatibili con un Sistema esperto.

Portando alle estreme conseguenze il discorso sull'automazione dell'attività amministrativa vincolata, l'automazione stessa renderebbe superflua l'attività provvedimentale della P.A. dal momento che questa verrebbe sostituita da un'operazione tecnica consistente nel trascrivere all'interno del computer il dettato normativo, utilizzando il linguaggio appropriato[33]. Il quesito provocatorio che

29. Vedi Caridi-Pellecchia 1986, p. 81 ss.

30. In tal senso anche Duni 2008, p. 54 ss.

31. Quando difettano parametri normativi *a priori* che possano fungere da premessa del ragionamento sillogistico, il giudice non "deduce" ma "valuta" se la decisione pubblica rientri o meno nella (ristretta) gamma delle risposte maggiormente plausibili e convincenti alla luce delle scienze rilevanti e di tutti gli altri elementi del caso concreto. È ben possibile per l'interessato – oltre a far valere il rispetto delle garanzie formali e procedimentali strumentali alla tutela della propria posizione giuridica e gli indici di eccesso di potere – contestare *ab intrinseco* il nucleo dell'apprezzamento complesso, ma in tal caso egli ha l'onere di metterne seriamente in discussione l'attendibilità tecnico-scientifica. Se questo onere non viene assolto e si fronteggiano soltanto opinioni divergenti, tutte parimenti plausibili, il giudice deve dare prevalenza alla posizione espressa dall'organo istituzionalmente investito (dalle fonti del diritto e, quindi, nelle forme democratiche) della competenza ad adottare decisione collettive, rispetto alla prospettazione individuale dell'interessato. Vedi Cons. Stato, sez. V, 9 maggio 2022, n. 3570; Cons. Stato, sez. VI, 15 luglio 2019, n. 4990.

32. Vedi Lucatuorto 2009.

33. Cfr. Fantigrossi 1992, p. 122 ss.

si vuole porre è se, a questo punto, avrebbe ancora ragione di esistere un apparato amministrativo dotato di funzionari pronti a beneficiare del potere di applicazione discrezionale delle norme, quando queste possano essere applicate in modo automatico per mezzo di una macchina[34]. Un discorso analogo interessa l'atto amministrativo in quanto espressione di volontà e di potere, dove anche i relativi problemi dell'incompetenza, della violazione di legge e dell'eccesso di potere verrebbero meno. A domande apocalittiche e a fantasiose suggestioni si propongono invece risposte tranquillizzanti.

Analizzando più in dettaglio gli elementi e la natura dell'attività vincolata, attraverso l'esame di entrambe le dottrine che ammettono o meno la distinzione dell'attività vincolata con quella discrezionale, si evince che il potere amministrativo sia un elemento imprescindibile anche per quelle fattispecie in cui il vincolo normativo esiste e che sia penetrante[35]. Quindi non si dovrebbe pensare all'automazione in termini di espansione della vincolatività delle norme, poiché non esiste l'equazione tra massimo vincolo e nessun potere in capo alla P.A. Il potere si frappone sempre tra la legge e l'atto, fungendo da catalizzatore per la trasformazione giuridica e l'amministrazione, dunque, in qualità di soggetto, rende attivo quel potere mediante una propria manifestazione di volontà.

Tuttavia gran parte del dibattito sulla legittimità e quindi sulla possibilità di automatizzare l'azione della P.A. si focalizza sulla discrezionalità amministrativa, oggetto di numerose interpretazioni[36].

Per discrezionale si intende l'attività i cui fini sono individuati in via generale dalla legge, mentre la scelta dei mezzi per conseguirli ricade sulla P.A.[37] La ragione per cui la legge si astiene, per così dire, dal pre-identificare anche i mezzi da impiegare risiede nel fatto che i conflitti tra gli interessi che animano la realtà quotidiana spesso non sono individuabili *ex ante* e sono imprevedibili. Discrezionalità significa, infine, scegliere tra un ventaglio di soluzioni ammesse dalla norma attributiva della competenza, in maniera concreta e a valle dell'iter procedimentale[38].

È doveroso fare una premessa: la fase riservata alle scelte ovvero all'esercizio del potere discrezionale non viene messa in dubbio né tantomeno eliminata dall'impiego del computer, mentre viene invece valorizzata in sede di preparazione del programma dove si riservano le scelte inerenti ad una serie di provvedimenti futuri, modificati da atti discrezionali in semplici accertamenti. L'autorità amministrativa, insomma, non si priva di alcuna facoltà e non delega alcun potere al sistema informatico. I compiti prima assegnati al funzionario pubblico ora vengono eseguiti dal sistema automatizzato, il cui maggiore contributo si registra in termini di uniformità, efficienza, e versatilità nelle operazioni e nelle attività[39]. L'esempio dei concorsi pubblici è emblematico in questo senso, in quanto per la correzione delle prove non vi sono margini discrezionali, dato che le prove sono di tipo ripetitivo e a risposta esatta o errata, perciò i risultati saranno rapidi ed obiettivi, teoricamente esenti da errori (se non per malfunzionamento della macchina).

Apparentemente l'idea di discrezionalità e la logica della programmazione computazionale sembrano essere agli antipodi, se non l'uno la negazione dell'altra. Da un lato vi è il software, che si fonda su due attività di formalizzazione, le quali in un secondo momento abbisognano di essere enunciate in un linguaggio formale dai significati univoci e secondo l'inflessibile schema dell'if-then; dall'altro abbiamo la discrezionalità, sinonimo di ponderazione e di scelta tra alternative lecite. Ciò non vuol dire che non esistano delle sfaccettature, delle declinazioni, dei passaggi intermedi tra l'uno e l'altra. Anzitutto esistono fattispecie a bassa discrezionalità, aventi limitate alternative possibili, dove è ipotizzabile disporre di un programma che prenda in considerazione, in sede di ponderazione, la presenza di esigue soluzioni e che sia capace di risolvere il contrasto, stabilendo *a priori*

34. Ancora Frosini 1983, p. 752.
35. Vedi per una panoramica delle problematiche, Cofrancesco-Borasi 2012, p. 112 ss.
36. Vedi Bassi 2001, p. 139 ss.; Satta 1969, p. 19 ss.; Sandulli 1984, p. 571 ss.; Villata 2005, p. 770 ss.
37. Vedi Duni, 2008, p. 72 ss.
38. *Ivi*, p. 45.
39. *Ibidem*.

gli interessi prevalenti. Esiste poi la possibilità di ricorrere ai sistemi esperti che affidano al computer l'individuazione di algoritmi allo scopo di ridurre la complessità della decisione da prendere[40].

D'altronde, può anche presentarsi il caso in cui non sia possibile indicare le istruzioni al momento della redazione del software, ad esempio, perché sono in corso di formazione, in attesa della promulgazione di una legge o dell'emanazione di una sentenza, e in tal caso il programma non indicherà il dato concreto bensì solamente l'indirizzo al quale la macchina dovrà ricercarlo[41].

Infine, non sempre è possibile informatizzare il procedimento nella sua interezza: questo avviene per casi più complicati, in cui parte del procedimento viene sottoposto ad informatizzazione, mentre il resto viene affidato al funzionario. In questo modo si opera una combinazione di mezzi informatici e manuali, che, probabilmente, rappresenta la modalità più opportuna per procedere alle attività che interessano la P.A.

Ma il rischio maggiore deriva dal fatto che l'amministrazione potrebbe limitare i propri poteri attraverso vincoli autoimposti tali da precludere qualsiasi margine di apprezzamento. L'esigenza allora sarà quella di distinguere, all'interno delle fattispecie di discrezionalità, quelle in cui la regola sia effettivamente non precisabile da quelle in cui tali regole potrebbero essere determinabili in base ad una casistica già presente nella norma, il cui scopo però non era esclusivamente semplificare il testo[42].

L'autonomia amministrativa non potrebbe travalicare il limite della delega in favore di sistemi per la decisione discrezionale automatizzata. In altri termini, se l'esercizio della discrezionalità venisse collocato a monte del procedimento, riducendo ad algoritmo i processi di acquisizione ed in particolare di ponderazione degli interessi in base ai parametri di ragionevolezza, logicità e congruità, sarebbe impedito l'esercizio della stessa all'interno del singolo procedimento, sbarrando la strada a qualsiasi spazio di apprezzamento dei presupposti fattuali e delle ragioni giuridiche che si presentano nelle varie ipotesi.

Per ridurre il rischio di un'eccessiva delega dell'esercizio di potere discrezionale soltanto la legge potrebbe intervenire, ad esempio, prevedendo che le amministrazioni, per ciascuna tipologia di procedimento, adottino atti amministrativi automatizzati in ordine all'attività discrezionale, magari mediante regolamento[43].

Sebbene per i procedimenti discrezionali sembri inevitabile l'ibridazione della procedura, tuttavia ciò non equivale ad affermare un minore livello di automazione[44]. All'interno della catena di operazioni in continuità automatica, si dischiude la fase valutativa degli interessi, che rappresenta il fulcro dell'attività discrezionale e che rimane ben salda nelle mani dell'operatore.

Secondo questo indirizzo dottrinale[45], che più spiccatamente auspica che l'informatizzazione e l'automazione divengano la regola da seguire per la strutturazione dell'attività amministrativa, il procedimento amministrativo è da intendersi come un flusso di automatismi e dovrebbe essere e rimanere "informatico" in ogni sua fase, in ogni suo momento. L'unica eccezione che si ammette è proprio in sede valutativa, dove l'opera compiuta dal fattore umano è imprescindibile e non delegabile alla macchina. Tuttavia, per accertare se un flusso sia interamente telematico, occorre confrontare sia i procedimenti analoghi che le interazioni con l'operatore sul piano quali-quantitativo. Induce ad errore paragonare un procedimento vincolato ad uno discrezionale al fine di ammettere che il primo raggiunga un livello di automazione maggiore. In aggiunta a questo si rischierebbe di considerare che dalla completa informatizzazione delle sotto-fasi dell'istruttoria, concepita come una sequela di azioni realizzate dagli apparati digitali senza bisogno del contributo umano, si giunga all'eliminazione del ruolo del titolare dell'organo. La realtà vuole invece che il responsabile del procedimento

40. Vedi Contaldo–Campara 2020.
41. *Ibidem*.
42. In tal senso Duni 2008, p. 85.
43. Vedi Contaldo–Campara 2020, p. 65 ss.
44. Vedi ancora Duni 2008, p. 48 ss.
45. Vedi Masucci 2011, p. 112.

mantenga il proprio ruolo anche nel contesto digitalizzato, senza che gli automatismi pregiudichino gli obblighi e i poteri riconosciuti *ex lege*. Oggetto del cambiamento saranno quindi le modalità ed i contenuti dell'attività istruttoria, poiché è impensabile che l'evoluzione del contesto amministrativo[46], da analogico a digitale, possa minare l'esigenza giuridica di un centro di responsabilità volto a dar conto di ciò che viene gestito dai sistemi informatici.

Venendo più nel dettaglio all'analisi dottrinale, nella maggioranza dei giuristi positivi regna uno scettiscismo di base in ordine alla possibilità di rendere automatizzata l'attività discrezionale, sottolineando che l'atto discrezionale, fondandosi sulla ragionevolezza umana, si conformerebbe ad una logica "opaca" non riconducibile a percorsi predeterminati o predeterminabili; contemporaneamente però si afferma che uno scenario diverso, considerata l'autorevolezza degli studiosi che sostengono tale tesi, non possa essere escluso *a priori*. Infatti con i progressi ottenuti dalla ricerca nel settore informatico sull'intelligenza artificiale (AI) si sono approfonditi i fondamenti teorici, le metodologie e le tecniche che favoriscono la progettazione di sistemi hardware e software volti a rendere l'elaboratore elettronico capace di performance apparentemente di pertinenza esclusiva dell'intelligenza umana[47]. Le connessioni del cervello umano vengono riprodotte nel calcolatore attraverso le c.d. reti neurali artificiali, cosicché la macchina dovrebbe essere messa nella condizione non solo di comprendere il linguaggio naturale ma anche di apprendere, di auto-perfezionarsi e infine di interpolare le informazioni incomplete.

Tuttavia si ritiene anche superabile la tesi generale dell'incompatibilità tra discrezionalità amministrativa ed elaborazione elettronica, potendo l'attività discrezionale-tecnica essere gestita mediante Sistemi Esperti he abbiano più opzioni logiche[48]. Per giungere a tale asserzione si considerano, da un lato, le analisi incentrate sulle modalità di impiego delle forme di autolimitazione volte a predeterminare, cioè in sede di programmazione del software, le modalità di esercizio della discrezionalità, dall'altro, le riflessioni generali sull'esigenza di interpretare la volontà insita nel provvedimento amministrativo come volontà procedimentale e sulla riferibilità all'autorità procedente anche della volontà dell'atto informatico[49]. Ciò detto, il programma, essendo meramente ausiliario al perseguimento dell'obiettivo che l'agente si è prefisso[50], può essere assunto anche per elaborare atti discrezionali dal punto di vista contenutistico. Gli atti così formulati risulteranno consciamente voluti quando colui che li sottoscrive abbia volontariamente adottato quel particolare software per produrre l'atto in quella determinata circostanza e in presenza di quei determinati presupposti.

Quando attraverso il software si introducono criteri validi ad orientare l'esercizio del potere nei singoli casi, allora c'è margine per una decisione automatizzata. Il potere discrezionale è allora esercitato a monte attraverso la predeterminazione di criteri e principi che l'elaboratore dovrebbe seguire nell'esame del materiale informativo e nell'adozione della decisione.

Più specificamente si parlerà dei c.d. sistemi esperti, ossia delle applicazioni di AI su base logica che utilizzano tecniche di "ragionamento" e conoscenze per risolvere problemi complessi, e che spiegano e motivano le ragioni della opzione prescelta[51].

È innegabile che automatizzare le decisioni discrezionali sia un'impresa ardua e piena di ostacoli, ma allo stesso tempo non impossibile[52]. Se in precedenza abbiamo osservato che la difficoltà di automatizzare le decisioni amministrative dipende dall'indeterminatezza dei concetti giuridici cui è possibile attribuire una molteplicità ed una diversità di significati, nel caso dei poteri discrezionali invece viene in rilievo un altro ordine di problemi

46. *Ibidem*.
47. Cfr. Sartor 2022, p. 94.
48. Delgado 2016, p. 146 ss.
49. Duni 2008, p. 65 ss.
50. Sartor–Loreggia 2022, p. 5 ss.
51. Faini 2019, p. 145 ss.
52. Masucci 2011, p. 115.

che concerne la molteplicità di scelte tra alternative di azione possibili[53]. Quando il potere discrezionale è un potere caratterizzato dalla non univocità delle modalità d'esercizio in riferimento al *se*, al come, al *quid* e al *quando* (o ad uno o a più d'uno di essi), di conseguenza la previsione normativa relativa al potere discrezionale non può essere, almeno in linea di principio, preventivamente riformulata in modo univoco e una volta per tutte. Inoltre, se la programmazione del computer presuppone che le previsioni normative debbano essere in via preventiva riformulate in un linguaggio formale dai significati univoci ed il medesimo processo decisionale debba essere rigidamente predeterminato una volta per tutte, si ricava che la pluralità e la diversità delle scelte tipiche del potere discrezionale collidono, in linea di principio, con la logica della programmazione decisionale del computer[54]. Questo perché la standardizzazione del procedimento è indispensabile per l'automatizzazione del medesimo, anche se una tale conclusione può essere superata dall'evoluzione tecnologica.

Oltre al possibile l'impiego dei c.d. sistemi esperti, la P.A. potrebbe fissare *ex ante* e in via generale i criteri in base ai quali il potere discrezionale dovrà essere esercitato di volta in volta nei singoli casi. In questo modo la predeterminazione dei criteri di esercizio della discrezionalità rende le scelte univoche ed obbligate[55]. Inoltre, trattandosi di esercizio anticipato di discrezionalità, in virtù del vincolo, non viene in luce alcuna omissione del potere discrezionale. Il software, in cui sono inserite le istruzioni concernenti i criteri di esercizio di detto potere, opera in qualità di norma interna che regola, in via preventiva, l'esercizio del potere discrezionale.

Anche l'intervento del responsabile del procedimento non pone particolari problemi. Dinanzi ad un atto vincolato, il sistema, generalizzando le procedure, assicura l'uniformità di trattamento e il rispetto delle norme che tipizzano il procedimento[56]. A fornire una motivazione esaustiva dell'atto sarebbe quindi il sistema, anche solo con un mero richiamo alla normativa. Se l'intera attività è predeterminata e realizzata dal sistema elettronico, al fattore umano non rimane che il compito di inserimento dei dati. I controlli inoltre potranno concentrarsi sull'idoneità del programma, e non tanto sulla correttezza delle singole operazioni. Mancando l'autore umano, per stabilire l'attribuzione della "paternità" ed eventuali responsabilità si deve necessariamente risalire a monte del procedimento fino al momento in cui il software è stato reputato rispondente ed idoneo ai criteri e ai fini tipizzati dalle norme[57].

Quando invece si ha un'attività discrezionale per la quale sia possibile l'automazione, le decisioni elaborate con l'informatizzazione necessitano di motivazione altrettanto automatica, in maniera non dissimile da quanto stabilito dalle norme generali per gli atti convenzionali.

Di fronte a procedimenti c.d. a bassa discrezionalità, l'interruzione del flusso degli automatismi è una pura eventualità dal momento che si possono prevedere opzioni di scelta basate sul verificarsi o meno di certe condizioni lasciate alla gestione autonoma degli elaboratori[58].

Se dunque l'istruttoria vede incrementato il proprio livello di automatizzazione, venendo meno tutta una serie di passaggi e adempimenti storicamente monopolizzati dall'azione umana, di riflesso l'attività svolta dall'operatore indossa una nuova veste. Anche nei procedimenti vincolati, per i quali è sufficiente accertare la rispondenza del caso concreto al cammino già delineato *in toto* dalla fattispecie normativa, il flusso digitale abbisogna del fattore umano: basti solo pensare alla progettazione, al controllo e alla supervisione dei processi automatici, stante che la responsabilità dell'attività amministrativa svolta e dei servizi resi all'utenza rimane naturalmente immutata[59]. La ragion d'essere dell'elemento umano risiede

53. *Ibidem*.
54. Faini 2019, p. 72 ss.
55. Duni 2008, p. 51 ss.
56. *Ibidem*.
57. Sartor 2022, p. 76.
58. Otranto 2018.
59. Sul tema vedi Cofrancesco–Borasi 2012.

poi, nei procedimenti discrezionali, nell'attività di valutazione-decisione e di bilanciamento degli interessi sottesi, spesso confliggenti, oltre che nella supervisione del regolare funzionamento dei sistemi e della completezza dei flussi.

È impensabile che l'esistenza e l'esigenza del momento valutativo possa essere addotto come motivo per negare la "automatizzabilità" di un procedimento discrezionale. Sta di fatto che la linea seguita dai recenti processi decisionali si muove verso un graduale restringimento della discrezionalità amministrativa, a partire dalle discipline legislative o regolamentari attributive di poteri, sempre più dettagliate, onnicomprensive, e inderogabili da parte delle autonomie locali.

Tutti questi elementi di riflessione posso essere presi in prestito per affrontare un'altra questione, ovverosia il fenomeno della "falsa discrezionalità"[60]. Stiamo parlando di un fenomeno caratterizzato dal fatto che alcuni soggetti pubblici gestiscono certe funzioni di propria competenza (adottando atti, assumendo decisioni e ponendo in essere determinate condotte) ritenendosi titolari di poteri discrezionali che, in realtà, non esistono[61]. Questa prassi cela un atteggiamento ostile nei confronti dell'impiego della tecnologia nella vita amministrativa. Sistemi informatici, piattaforme digitali, automazioni, etc., sono visti come nemici usurpatori di un qualcosa che si è da sempre percepito come proprio. Tuttavia, e aggiungiamo fortunatamente, non tutti all'interno della P.A. sono di questo parere.

Ormai la libera valutazione è molto ridimensionata, e ciò è dovuto in parte al legislatore, il quale ha ridotto i margini di apprezzamento valutativo, incanalando le procedure in percorsi vincolati, in parte alla diffusione di regolamenti e programmazioni sempre più esaurienti. Segue che quando ci si trova dinanzi ad una situazione foriera di applicazioni diverse, benché legittime, per evitare di incorrere nel rischio di differenziazioni, si opta per una disciplina preventiva di natura generale ed astratta, cosicché si riduce la gamma delle possibili scelte nei casi concreti oggetto di provvedimenti puntuali[62].

5. Sistemi Esperti: un'applicazione consolidata per le attività amministrative non discrezionali

I sistemi esperti amministrativi rappresentano pertanto una soluzione interessante: questi rispondono a domande sulla qualificazione giuridica di una determinata circostanza (violazione al codice della strada oppure mancato pagamento di una tipologia di tributo). Solitamente, un sistema di questo genere riceve come input la descrizione di un caso e come output fornisce la sua qualificazione giuridico-amministrativa. I sistemi di analisi giuridico-amministrativa sono interattivi e ciò vuol dire che il funzionario della P.A., dialogando con il sistema, specifica la descrizione del caso e il programma ne deriva un effetto giuridico, applicando le informazioni presenti nella sua base di conoscenza. Di tali strumenti possono usufruire tanto il giurista "generico" (studioso, docente, avvocato) quanto le pubbliche amministrazioni, ad esempio per il calcolo tributario, salariale, pensionistico, ecc., a beneficio della comunità. I sistemi esperti giuridici diventano necessari per le attività legali, che constatano di un impegno attivo della conoscenza, non rigidamente predeterminato. Impiegando una rappresentazione formale della conoscenza del diritto, i sistemi esperti giuridici riproducono una certa attività giuridica in un software. Da ciò deriva che il processo di elaborazione giuridico-amministrativa è un processo razionalizzabile, almeno parzialmente, e che è possibile individuare e riprodurre le fonti del diritto (soprattutto circolari amministrative, importanti per la funzionalità degli uffici della P.A.) ricorrendo ad un linguaggio manipolabile dall'elaboratore. Allo stesso tempo, però, non è operazione semplice ed immediata la definizione dell'intera realtà amministrativa da acquisire. Motivo ne è il fatto che la conoscenza necessaria a risolvere problemi e formulare decisioni racchiude sia nozioni ricavabili da fonti scritte ("conoscenze pubbliche") sia elementi non codificati in testi ufficiali e derivanti dall'esperienza ("conoscenze private")[63]. Il ricorso al sistema esperto giuridico-amministrativo si

60. Fracchia–Occhiena 2020, p. 137 ss.

61. Taddei Elmi–Marchiafava–Unter 2021, p. 102 ss.

62. Iaselli 1998, p. 74 ss.

63. Cfr. Mariani 1989, p. 72 ss.

concreta non nella lettura di documenti registrati nella sua memoria – ciò che avviene con i più conosciuti sistemi di documentazione giuridica automatica –, bensì come mezzo capace di eseguire calcoli e deduzioni logiche riguardo le conoscenze di cui è dotato.

È possibile classificare i sistemi esperti giuridico-amministrativi sulla scorta di tre elementi: l'oggetto (la conoscenza), il metodo (la rappresentazione) e gli obiettivi (l'utilizzo reale). Per quanto concerne il primo, l'oggetto di un sistema esperto giuridico-amministrativo può consistere in un momento dell'attività giuridica, come ad esempio la produzione normativa (ad esempio di circolari), la ricerca dei precedenti o delle conclusioni giuridiche deducibili dalla conoscenza di cui il sistema è dotato. Il livello di specializzazione del sistema esperto implicherà, naturalmente, scelte differenti riguardo alla tipologia di conoscenze le quali, a loro volta, richiederanno diverse tecniche di rappresentazione. In definitiva, la configurazione dei sistemi esperti giuridici dipenderà, allora, dalla combinazione di vari parametri. In virtù del fatto che al termine "conoscenza" è possibile attribuire significati diversi a seconda del rapporto tra la sua fonte (l'esperto umano o i testi scritti) e la relativa rappresentazione data dalla macchina, in dottrina si è pervenuti ad una quadripartizione dei sistemi esperti giuridici[64].

In primo luogo, vi è il sistema esperto c.d. classico, il quale simula il comportamento del funzionario pubblico e lo aiuta a prendere decisioni, senza mai ad esso sostituirsi. Tale sistema ha scarsissima conoscenza legislativa, poiché simula il processo di soluzione legale piuttosto che il ragionamento esplicito sulla legge stessa. È interessante far notare che questi sistemi sono in grado di rilevare l'esistenza di alcuni conflitti e, dunque, di avvisare l'utente circa le condotte "probabili". Ed è agevole capire che proprio questo è uno dei tratti precipui dei sistemi esperti: fornire spiegazioni e giustificazioni alle proprie conclusioni, mostrando le assunzioni su cui si sono fondate, ovvero l'insieme di argomenti che possono essere costruiti dai fatti di un caso specifico, ponendone alcuni a favore ed altri contro una particolare soluzione. Spetterà, poi, al funzionario pubblico valutare, confrontare ed accettarne liberamente uno, guardando al ventaglio di opzioni alternative prospettate dal sistema esperto.
Passando alla seconda classe di sistema esperto, questa, anziché costituire il processo di risoluzione di problemi amministrativi, inerisce al contenuto di un determinato e delimitato dominio legislativo. Detto altrimenti, trattasi di un sistema esperto che rappresenta l'interpretazione data da un esperto umano di una fattispecie rapportandola ad un testo normativo[65].

Nella logica dei sistemi esperti vi è il linguaggio di rappresentazione più efficace, visto che le risposte fornite derivano logicamente dalle informazioni contenute nella base di conoscenza oppure da quelle combinate con le informazioni aggiunte dall'utente. Queste ultime vanno a formare un database esterno, cui il sistema esperto ricorre quando abbisogna di alcuni dati per il processo di soluzione del problema. Il sistema esperto, perciò, dà spiegazioni che corrispondono a prove logiche scaturite dalla conoscenza del sistema combinata con quella aggiunta dall'utente[66].

Il terzo tipo di sistema esperto si basa sulla logica, pur tendendo a rappresentare in modo diretto una parte di legislazione, senza rifarsi all'interpretazione di un esperto umano. In un primo tempo l'idea era quella di formalizzare tutte le clausole della disposizione normativa (legge, regolamento, circolari del MEF) separatamente – anziché lo stesso nella sua interezza –, cosicché più funzionari potessero concentrarsi su singole parti, accomunate solamente dal vocabolario dei termini usati nella formalizzazione[67]. Il risultato, però, fu quello di una rappresentazione non accurata ed eccessivamente semplificata, il che portò a dover concepire il testo normativo come un'unità inscindibile. Questa classe di sistemi esperti si prefiggeva come obiettivo principale la rappresentazione dell'esatta volontà del legislatore; sarebbe riduttivo vedere la legge solo in questa prospettiva visto che essa, invero, si sostanzia anche e soprattutto nell'interpretazione data dalle autorità esecutive.

64. Fameli–Nannucci 1989, p. 122 ss.

65. Cammelli–Socci 1991, p. 45 ss.

66. Caridi 1985, p. 71 ss.

67. Fameli 1995, p. 191 ss.; Durante 2012, p. 84 ss.

Infine, il quarto tipo di sistema esperto giuridico-amministrativo combina regole di formalizzazione di regolamenti e incidenze supplementari basate sull'opinione di un esperto[68]. L'utente deve fornire informazioni concernenti proprie circostanze e ha facoltà di sperimentare diverse interpretazioni del sistema finché non pervenga ad una (o più) conclusione a lui congeniale; questi sono i sistemi basati su "modelli concettuali profondi", che sono capaci di conoscere e quindi trattare anche i concetti contenuti nelle regole, nonché di arrivare alla scelta delle regole pertinenti al caso specifico e alla giustificazione del ragionamento in modo intelligente (ad esempio una gradualità della sanzione amministrativa).

Premesso che l'impiego dei sistemi sia a sostegno e mai in sostituzione dell'attività del funzionario pubblico, si può ipotizzare una serie di ambiti applicativi che richiede l'individuazione di specifiche funzioni di cui dotare i sistemi esperti[69].

Perciò, a seconda della categoria di informazioni trattate dal computer, si possono distinguere sistemi esperti di consulenza o di aiuto alla decisione e sistemi per il reperimento "intelligente" in database. Se i primi hanno a che fare solo con conoscenza rielaborata, i secondi possono gestire anche informazioni strutturate in una base di dati, ricorrendo ad una minima parte di conoscenza formale prevalentemente funzionale alla raccolta delle informazioni stesse.

Lo sviluppo di quest'ultima tipologia di sistema ha proceduto di pari passo con lo sviluppo dei sistemi esperti ed indipendentemente da essi. La necessità era quella di potenziare i sistemi informatici documentari amministrativi tradizionali, dotandoli di sistemi intelligenti per il reperimento delle informazioni: per un verso, si è operato nella direzione di estendere le funzionalità degli attuali database per soddisfare nuovi domini di applicazione; per l'altro, si sono sfruttate le potenzialità offerte da ambienti evoluti di programmazione. In particolare a livello della c.d. informatica giuridica di tipo documentario, si è notato che i sistemi di informazione tradizionali (banche dati amministrative) richiedono all'utente una buona conoscenza delle funzioni di ricerca, non assicurando al contempo una ricerca completa e precisa. In aggiunta, nello sviluppo della documentazione amministrativa, si stagliano problemi non superabili con le tecniche di reperimento tradizionali, basate sulla ricerca testuale[70].

Il *modus operandi* di un sistema esperto di reperimento (come quello dell'amministrazione finanziaria che effettua i cosiddetti "incroci delle banche dati") vede, solitamente, l'attivazione di un meccanismo comparativo fra la richiesta del funzionario dell'Agenzia delle Entrate e le informazioni detenute dalle diverse banche dati. Ai fini del confronto, entrambe vengono fatte confluire in una rappresentazione interna con un comune formalismo predefinito. Il ricorso al meccanismo inferenziale è volto a stabilire una qualche relazione di somiglianza fra di esse e ad individuare, perciò, l'informazione pertinente. Esemplificando, in un database dell'Amministrazione finanziaria, la risposta fornita al quesito da parte di un sistema di reperimento non sarà la deduzione della ricerca richiesta, bensì i precedenti amministrativi affini al caso in esame, che consentirà al funzionario pubblico di meglio redigere l'atto amministrativo conseguente.

Relativamente ai sistemi misti, questi operano, da un lato, combinando conoscenza e, dall'altro, rintracciando informazioni. Gli ambienti di programmazione più evoluti permettono di perfezionare ulteriormente il collegamento fra sistema esperto e database; nel processo decisionale si impiegano anche i contenuti della base di dati, e ciò consente un continuo aggiornamento della base di conoscenza.

In ordine ai sistemi esperti di aiuto alla decisione amministrativa (in particolare modo per le sanzioni di competenza degli Uffici Territoriali di Governo-ex Prefetture), invece, essi si configurano con una generica funzione di consulenza – sempre specificabile –, a seconda che sia indirizzata a fornire risposte in termini previsionali, valutativi o decisionali.

Diversi sono gli aspetti che vanno a definire le caratteristiche funzionali di un sistema esperto: si rileva come differenti strutture e problemi nella pratica amministrativa siano, invece, strettamente

68. *Ibidem*.

69. Sartor 2020.

70. Contaldo 2002, p. 548 ss.

correlati ad ambiti applicativi dei sistemi esperti giuridici, alle sue differenti metodologie e funzioni. Come si diceva in precedenza, una legge non vive esclusivamente in norme scritte, ma anzi è affiancata o, quanto meno, risente delle decisioni prese per casi precedenti delle singole amministrazioni. Allora si può affermare che la struttura giuridica conduce ad un rovesciamento di interessi ed anche ad un diverso punto di partenza. Tale distinzione è suscettibile di influenzare la progettazione di Sistemi Esperti che, oltre a fornire aiuto al processo decisionale del funzionario pubblico, intendano analizzare il sistema amministrativo stesso, sia nella dimensione statica o dinamica, sia nel ragionamento. Generalmente, i sistemi progettati per l'analisi dei problemi giuridici richiedono una copertura, a livello di conoscenza, più estesa e articolata rispetto ai sistemi di reperimento concettuale di informazioni o quelli di consulenza automatica[71]. Questi sistemi devono essere idonei a riprodurre l'attività del funzionario pubblico, che utilizza forme di conoscenza diversa con processi mentali differenti; sul piano informatico la conoscenza normativa sembra trattata in modo appropriato impiegando processi deduttivi, mentre la conoscenza giurisprudenziale privilegia per eccellenza ragionamenti di tipo analogico.

Riferimenti bibliografici

A.C. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

U. Allegretti (1998), *Amministrazione pubblica e Costituzione*, Cedam, 1998

U. Allegretti (1993), *Imparzialità e buon andamento*, in "Digesto delle discipline pubblicistiche", vol. VIII, Utet, 1993, p. 864 ss.

U. Allegretti (1965), *L'imparzialità amministrativa*, Cedam, 1965

M. Allena (2012), *La rilevanza dell'art. 6, par. 1, CEDU per il procedimento e il processo amministrativo*, in "Diritto processuale amministrativo", 2012, n. 2

C. Amirante (2004), *Principles, Values, Rights, Duties, Social Needs in The Interpretation of the Constitution*, in J. Nergelius, P. Policastro, K. Urata, (eds.), "Challenges of Multilevel Constitutionalism", Proceedings of the IVR 21st World Congress, 12-18 August 2003, Cracow, 2004

S. Arcieri (2019), *Bias cognitivi e decisione del giudice: un'indagine sperimentale*, in "Diritto penale e Uomo", 2019, n. 4

G. Arena, G. Corso, G. Gardini et al. (a cura di) (2008), *La trasparenza amministrativa*, Giuffrè, 2008

P. Barile (1958), *Il dovere di imparzialità della pubblica amministrazione*, in AA.VV., "Scritti Giuridici in memoria di Piero Calamandrei", vol. IV, Cedam, 1958

A. Bartolini, S. Fantini, G. Ferrari (2010), *Codice dell'azione amministrativa e delle responsabilità*, Neldiritto Editore, 2010

N. Bassi (2001), *Principio di legalità e poteri amministrativi impliciti*, Giuffré, 2001

A. Cammelli, F. Socci (1991), *Caratteristiche e finalità di un sistema esperto nel diritto: proposta di un sistema giuridico integrato*, in "Informatica e diritto", 1991, n. 1-3

A. Capdiferro Villagrasa (2020), *La inteligencia artificial del sector publico: desarrollo y regulation de la actuacion adiministrativa inteligente en la cuarta revolucion industrial*, in "Revista del los Estudios Drecho y Ciencia Politica", 2020

71. Orofino–Gallone 2020, p. 1738.

R. Caranta (2008) (a cura di), *Interest Representation in Administrative Proceedings*, Jovene, 2008

L. Carbone (2023), *L'algoritmo e il suo giudice*, in www.giustizia.amministrativa.it, 2023

G. Caridi, S. Pellecchia (1986), *Automazione della ricerca giuridica e sistemi esperti*, FrancoAngeli, 1986

F. Caringella, M. Protto (a cura di) (2009), *Il nuovo procedimento amministrativo*, Dike Giuridica, 2009

L. Carlassare (1974), *Amministrazione e potere politico*, Cedam, 1974

E. Carloni (2014), *L'amministrazione aperta: regole strumenti limiti dell'open government*, Maggioli, 2014

S. Cassese (2011), *Il diritto alla buona amministrazione*, in "Studi in onore di Alberto Romano", vol. I, Editoriale Scientifica, 2011

S. Cassese (2007), *La partecipazione dei privati alle decisioni pubbliche*, in "Rivista trimestrale di diritto pubblico", 2007, n. 1

S. Cassese (1973), *Imparzialità amministrativa e sindacato giurisdizionale*, Giuffrè, 1973

A. Celotto (2019), *I robot possono avere diritti?*, in "BioLaw Journal", 2019, n. 1

P. Cerbo (2007), *Potere organizzativo e modello imprenditoriale nella pubblica amministrazione*, Cedam, 2007

A. Cerri (2009), *Istituzioni di diritto pubblico*, Giuffrè, 2009

A. Cerri (2006), *Uguaglianza (principio costituzionale di)*, voce in "Enciclopedia giuridica Treccani", aggiornamento XIV, 2006

A. Cerri (1998), *Principi di legalità, imparzialità, efficienza*, in L. Lanfranchi (a cura di), "Garanzie costituzionali e diritti fondamentali", Istituto della Enciclopedia Italiana, 1998

A. Cerri (1992), *L'eguaglianza giuridica nei rapporti interprivati*, in "Foro italiano", 1992, n. 5

A. Cerri (1973), *Imparzialità ed indirizzo politico della pubblica amministrazione*, Cedam, 1973

A. Cerri, G. Galeotti (a cura di) (2012), *Efficacia ed efficienza dell'azione pubblica*, Carocci, 2012

G. Chirichiello (2000), *I fondamenti economici dell'ordine giuridico del mercato*, in N. Irti (a cura di), "Il dibattito sull'ordine giuridico del mercato", Laterza, 2000

G. Cofrancesco, F. Borasi (2012), *Le figure della discrezionalità amministrativa*, Giappichelli, 2012

S. Cognetti (2010), *Principio di proporzionalità*, Giappichelli, 2010

G.D. Comporti (2001), *Tempus regit actionem. Contributo allo studio del diritto intertemporale dei procedimenti amministrativi*, Giappichelli, 2001

A. Contaldo (2002), *La ricerca normativa e giurisprudenziale su Internet: lo stato dell'arte per una rinnovata information retrieval*, in "Giurisprudenza di merito", 2002, n. 3

A. Contaldo, F. Campara (2020), *I Sistemi legali esperti e Intelligenza artificiale*, in G. Taddei Elmi, A. Contaldo (a cura di), "Intelligenza artificiale. Algoritmi giuridici, ius condendum o fantadiritto?", Pacini, 2020

A. Contaldo, M. Gorga (2006), *E-law. Le professioni legali, la digitalizzazione delle informazioni giuridiche e il processo telematico*, Rubbettino, 2006

F. Costantino (2012), *Autonomia dell'amministrazione e innovazione digitale*, Editoriale Scientifica, 2012

G. D'Auria (2009), *Dirigenti pubblici: garanzie nel conferimento degli incarichi e tutela reale contro licenziamenti illegittimi*, in "Foro italiano", 2009, n. 11

G. De Minico (2011), *Diritti Regole Internet*, in "Costituzionalismo.it", 2011, n. 2

I.M. Delgado (2016), *La riforma dell'amministrazione digitale: un'opportunità per ripensare la pubblica amministrazione*, in S. Civitarese Matteucci, L. Torchia (a cura di), "La tecnificazione", vol. IV, Firenze University Press, 2016

M. Deodati (2017), *Il nuovo procedimento amministrativo digitale*, Maggioli, 2017

G. Della Cananea (2008), *I procedimenti amministrativi dell'Unione Europea*, in M.P. Chiti, G. Greco (a cura di), "Trattato di diritto amministrativo europeo", Giuffrè, 2008

G. Della Cananea (a cura di) (2007), *I principi dell'azione amministrativa nello spazio giuridico globale*, Editoriale Scientifica, 2007

G. Duni (2008), *L'amministrazione digitale. Il diritto amministrativo nella evoluzione telematica*, Giuffrè, 2008

G. Duni (1978), *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, in "Rivista Amministrativa della Repubblica Italiana", 1978, n. 6

M. Durante (2012), L'*intelligenza artificiale nella prospettiva dell'informatica giuridica*, in M. Durante, U. Pagallo (a cura di), "Manuale di informatica e di diritto delle nuove tecnologie", Utet, 2012

W.D. Eggers (2017), *Pubblica amministrazione digitale* (trad. it.), Hoepli, 2017

F. Faini (2019), *Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico*, in "Biolaw Journal", 2019, n. 1

G. Falcon (a cura di) (2008), *Il procedimento amministrativo nei diritti europei e nel diritto comunitario. Ricerche e tesi in discussione*, Cedam, 2008

E. Faletti (2023), *Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi*, in "Il diritto dell'informazione e dell'informatica", 2023, n. 1

E. Fameli, R. Nannucci (1989), *Sviluppo dei sistemi esperti in campo giuridico*, in A.A. Martino, "Sistemi esperti applicati al diritto", Giuffrè, 1989

U. Fantigrossi (1992), *Automazione e pubblica amministrazione*, il Mulino, 1992

R. Ferrara (2011), *L'interesse pubblico al buon andamento della pubblica amministrazione tra forma e sostanza*, in "Studi in onore di Alberto Romano", vol. I, Editoriale Scientifica, 2011

F. Figorilli (1996), *Il contraddittorio nel procedimento amministrativo*, Edizioni Scientifiche Italiane, 1996

L. Floridi (2014), *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli, 2014

F. Fracchia, M. Occhiena (2020), *Le norme interne: potere, organizzazioni e ordinamenti. Spunti per definire un modello teorico concettuale generale applicabile anche alle reti, ai social e all'intelligenza artificiale*, Editoriale Scientifica, 2020

T.E. Frosini (2022), *La privacy nell'era dell'intelligenza artificiale*, in "DPCE on line", 2022, n. 1

V. Frosini (1983), *L'informatica e la pubblica amministrazione*, in "Rivista trimestrale di diritto pubblico", 1983, n. 2

H. Fry (2018), *Hello World. Esseri umani nell'era delle macchine* (trad. it.), Bollati Boringhieri, 2018

D.-U. Galetta (2022), *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal PNRR e problemi ancora da affrontare*, in "federalismi.it", 2022, n. 3

G. Gallone (2023), *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione tra procedimento e processo*, Cedam, 2023

R. Garofoli (a cura di) (2009), *La nuova disciplina del procedimento e del processo amministrativo*, Neldiritto Editore, 2009

M.S. Giannini (2000), *Istituzioni di diritto amministrativo*, Giuffrè, 2000

M.S. Giannini (1939), *Il potere discrezionale della pubblica amministrazione. Concetto e problemi*, Giuffrè, 1939

M. Iaselli (1998), *I sistemi esperti legali. Intelligenza artificiale e diritto*, Simone, 1998

P. Lazzara (2008), *I procedimenti amministrativi ad istanza di parte*, Jovene, 2008

P.L.M. Lucatuorto (2009), *Teoria e modelli del diritto per il ragionamento giuridico automatico*, LED Edizioni Universitarie, 2009

P.L.M. Lucatuorto (2006), *Artificial Intelligence and Law: Judicial Applications of Expert Systems* (*Intelligenza artificiale e diritto: le applicazioni giuridiche dei Sistemi Esperti*), in "Ciberspazio e Diritto", 2006, n. 2

F. Luciani (2022), *Brevi note sull'innovazione tecnologica come strumento di buona amministrazione*, in "La cittadinanza europea", 2022, n. 2

E.M. Marenghi (2009), *Procedimenti e processualprocedimento*, Cedam, 2009

P. Mariani (1989), *Intelligenza artificiale e sistemi esperti*, in P. Mariani, D. Tiscornia (a cura di), "Sistemi esperti giuridici. L'intelligenza artificiale applicata al diritto", FrancoAngeli, 1989

P. Mariani, D. Tiscornia (a cura di), (1989), *Sistemi esperti giuridici. L'intelligenza artificiale applicata al diritto*, FrancoAngeli, 1989

D. Marongiu (2005), *L'attività amministrativa automatizzata*, Maggioli, 2005

A. Massera (a cura di) (2008), *Le tutele procedimentali. Profili di diritto comparato*, Jovene, 2008

A. Masucci (2011), *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli, 2011

A. Masucci (2000), *Il documento amministrativo informatico*, Maggioli, 2000

B.G. Mattarella (2009), *I procedimenti*, in L. Torchia, (a cura di), "Il sistema amministrativo italiano", il Mulino, 2009

B.G. Mattarella (2005), *Informazione e comunicazione amministrativa*, in "Rivista trimestrale di diritto pubblico", 2005, n. 1

F. Merusi (a cura di) (2009), *Lezioni sul procedimento amministrativo*, Plus - Università di Pisa, 2009

G. Morbidelli (2005), *Il procedimento amministrativo*, in L. Mazzarolli, G. Pericu, A. Romano, F.A. Roversi Monaco, F.G. Scoca, (a cura di), "Diritto amministrativo", Monduzzi Editoriale, 2005

G. Morbidelli (1998), *Il procedimento amministrativo*, Giuffrè, 1998

A. Natalini (2022), *Come il passato influenza la digitalizzazione della amministrazioni pubbliche*, in "Rivista trimestrale di diritto pubblico", 2022, n. 1

M. Natoli (2003), *L'attività informatizzata della pubblica amministrazione*, in "Rivista Amministrativa della Repubblica Italiana", 2003, n. 9

C. Notarmuzi (2008), *Il procedimento amministrativo informatico*, in E. De Giovanni, C. D'Orta (a cura di), "Diritto pubblico delle ICT", Giuffrè, 2008

M. Occhiena (2002), *Situazioni giuridiche soggettive e procedimento amministrativo*, Giuffrè, 2002

A.G. Orofino, G. Gallone (2020), *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in "Giurisprudenza italiana", 2020, n. 7

P. Otranto (2018), *Decisione amministrativa e digitalizzazione della p.a.*, in "federalismi.it", 2018, n. 2

M. Palma (2022), *Gli algoritmi dell'amministrazione pubblica e l'amministrazione pubblica degli algoritmi*, in "Rivista italiana di informatica e diritto", 2022, n. 2

N. Paolantonio (2021), *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi. (Sul controllo giudiziario delle "decisioni algoritmiche")*, in "Diritto amministrativo", 2021, n. 4

F. Pizzetti (2018), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018

N. Rangone (2021), *Le pubbliche amministrazioni alla prova dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

A.M. Sandulli (1984), *Manuale di diritto amministrativo*, xiv ed., Jovene, 1984

M.A. Sandulli (a cura di) (2011), *Codice dell'azione amministrativa*, Giuffrè, 2011

G. Sartor (2022), *Intelligenza artificiale e diritto*, Giappichelli, 2022

G. Sartor (2020), *L'intelligenza artificiale e il diritto*, in "Rivista di filosofia del diritto", 2020, n. 1

G. Sartor (2002), *Gli agenti software: nuovi soggetti del ciberdiritto?*, in "Contratto e impresa", 2002, n. 2

G. Sartor, A. Loreggia (2022), *L'Intelligenza Artificiale nella moderazione del digitale*, in "Sistemi intelligenti", 2022, n. 1

F. Satta (1969), *Principio di legalità e pubblica amministrazione nello Stato democratico*, Cedam, 1969

G. Taddei Elmi, S. Marchiafava, A. Unter (2021), *Responsabilità civile, personalità giuridica dell'intelligenza artificiale*, in "i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, n. 2

L. Torchia (2023), *Lo Stato digitale. Una introduzione*, il Mulino, 2023

A. Usai (1993), *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in "Il diritto dell'informazione e dell'informatica", 1993, n. 1

R. Villata, (2005), *L'atto amministrativo*, in L. Mazzarolli, G. Pericu, A. Romano et al. (a cura di), "Diritto Amministrativo", v ed., Monduzzi, 2005

S. Zuboff (2019), *Il capitalismo della sorveglianza* (trad. it.), Luiss University Press, 2019