RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da Sebastiano Faro e Marina Pietrangelo

Anno IV, n. 2/2022 • Periodicità semestrale • ISSN 2704-7318
Periodico telematico: www.rivistaitalianadiinformaticaediritto.it
Direzione e Redazione: Istituto di Informatica Giuridica e Sistemi Giudiziari • Via dei Barucci 20 - 50127 Firenze

In questo numero

Gli algoritmi pubblici tra legalità e partecipazione

SEZIONE MONOGRAFICA

a cura di
B. Ponti

2 2022

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto
Periodico internazionale del CNR-IGSG

Anno IV • n. 2/2022 • Periodicità semestrale
www.rivistaitalianadiinformaticaediritto.it

Direzione Sebastiano Faro (IGSG-CNR) e Marina Pietrangelo (IGSG-CNR)

Comitato di direzione Federigo Bambi (Univ. Firenze), Elda Brogi (European University Institute), Davide Carnevali (IGSG-CNR), Gian Luca Conti (Univ. Pisa), Enrico Francesconi (IGSG-CNR), Antonio Iannuzzi (Univ. Roma-Tre), Erik Longo (Univ. Firenze), Stefano Pietropaoli (Univ. Firenze), Francesco Romano (IGSG-CNR)

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

Comitato scientifico dei corrispondenti stranieri Y. Amoroso (C), T.J.M. Bench Capon (GB), D. Bourcier (F), W.E. Boyd (USA), V. De Mulder (NL), J. Dumortier (NL), F. Galindo (E), A. Gardner (USA), T. Gordon (D), G. Greenleaf (AUS), O.P. Hance (L), W. Kilian (D), F. Lachmayer (A), P. Leith (IRL), E. Mackaay (CAN), A. MacIntosh (GB), P. Maharg (GB), J. Mayor (USA), L.T. McCarty (USA), F. Novak (CZ), A. Paliwala (GB), A.E. Perez-Luño (E), R. Petrauskas (LT), L. Philipps (D), Y. Poullet (B), A. Saarempaa (FIN), E. Schweighofer (A), P. Seipel (S), R. Susskind (GB), W.R. Svoboda (A), H. Yoshino (J), T. Van Engers (NL), M.A. Wimmer (A), R. Winkels (NL), J. Zeleznikow (AUS)

Esperti per la valutazione Fulvia Abbondante (Univ. Napoli-Federico II), Enrico Albanesi (Univ. Genova), Maria Romana Allegri (Univ. Roma-Sapienza), Marco Bassini (Univ. Milano-Bocconi), Raffaella Brighi (Univ. Bologna), Simone Calzolaio (Univ. Macerata), Giuseppe Cammarota (Univ. Cagliari), Gianluigi Ciacci (Univ. Roma-LUISS), Sofia Ciuffoletti (Univ. Firenze), Melania D'Angelosante (Univ. Chieti), Isaac Martín Delgado (Universidad de Castilla-La Mancha), Maria Vittoria Dell'Anna (Univ. Salento), Fabio Dell'Aversana (Univ. Cassino e Lazio Meridionale), Francesco di Ciommo (Univ. Roma-LUISS), Rossana Ducato (Univ. Trento), Fernanda Faini (Univ. Pisa), Elisabetta Frontoni (Univ. Roma-Tre), Paolo Galdieri (Univ. Napoli-Federico II), Riccardo Gualdo (Univ. Tuscia), Paolo Guarda (Univ. Trento), Ilaria Kutufà (Univ. Pisa), Alessandro Lovari (Univ. Cagliari), Gianclaudio Malgieri (Free University of Brussels – VUB), Fabio Martinelli (IIT-CNR), Daniele Marongiu (Univ. Cagliari), Letizia Materassi (Univ. Firenze), Giuseppe Mobilio (Univ. Firenze), Matteo Monti (Univ. Roma-LUISS), Angelo Giuseppe Orofino (Univ. LUM), Erica Palmerini (Scuola Superiore Sant'Anna), Saulle Panizza (Univ. Pisa), Anna Papa (Univ. Napoli-Parthenope), Viviana Patti (Univ. Torino), Nicola Pettinari (Univ. Perugia), Giovanni Piccirilli (Univ. Roma-LUISS), Benedetto Ponti (Univ. Perugia), Cecilia Robustelli (Univ. Modena e Reggio Emilia), Andrea Rossetti (Univ. Milano-Bicocca), Simone Scagliarini (Univ. Modena e Reggio Emilia), Caterina Sganga (Scuola Superiore Sant'Anna), Maurizio Tesconi (IIT-CNR), Marco Torre (Univ. Firenze), Emilio Tosi (Univ. Milano-Bicocca), Giuseppe Vaciago (Univ. Insubria), Giulia Venturi (ILC-CNR)

Segreteria di redazione Simona Binazzi
Elaborazione dei testi Giuseppina Sabato
Responsabile del sito web Elisabetta Marinai

Direzione e Redazione
IGSG/CNR
Via dei Barucci, 20 • 50127 Firenze
tel. 055 43995 • fax 055 4399605 • RivistaRIID@igsg.cnr.it • www.rivistaitalianadiinformaticaediritto.it

Direttore responsabile Sebastiano Faro

Registrazione presso il Tribunale di Roma al n. 127/2019

Indice

Sezione monografica

GLI ALGORITMI PUBBLICI TRA LEGALITÀ E PARTECIPAZIONE
a cura di Benedetto Ponti

5 **BENEDETTO PONTI**
Introduzione

7 **ALESSANDRO PUZZANGHERA**
La sfida tecnologica alla legalità amministrativa

15 **WALTER DIDIMO • LUCA GRILLI • GIUSEPPE LIOTTA • FABRIZIO MONTECCHIANI**
Efficient and trustworthy decision making through human-in-the-loop visual analytics: A case study on tax risk assessment

23 **FRANCESCO MERENDA**
Legalità, algoritmi e corruzione: le tecniche di intelligenza artificiale potrebbero essere utilizzate *nel* e *per* il sistema di prevenzione della corruzione?

39 **MATTEO PALMA**
Gli algoritmi dell'amministrazione pubblica e l'amministrazione pubblica degli algoritmi

55 **MATTEO FALCONE**
Bisogni conoscitivi delle amministrazioni e principio di legalità: quale predeterminazione delle scelte conoscitive pubbliche?

67 **LUIGI PREVITI**
La gestione del rischio informatico nella decisione amministrativa robotica

Studi e Ricerche

75 **SEBASTIANO FLAMINIO**
Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act

95 **DANIELE CHIAPPINI**
Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'*Artificial Intelligence Act* dell'Unione europea

109 **Vittoria Sveva Zilia Bonamini Pepoli**
Profili di contrasto al cybercrime *in iure condito* e *de iure condendo*

Osservatorio su
Intelligenza Artificiale e diritto
coordinato da Giancarlo Taddei Elmi

123 **Giancarlo Taddei Elmi, Sofia Marchiafava**
Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina

141 **Casimiro Coniglione**
Recensione a: Barbara Giovanna Bello, Laura Scudieri (a cura di), *L'odio online: forme, prevenzione e contrasto*, Torino, Giappichelli, 2022

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0091

Gli algoritmi pubblici: quale legalità e quale partecipazione? Introduzione

Benedetto Ponti

Nell'ambito dell'ampio ed articolato Convegno internazionale "Legalità e Partecipazione. Tendenze, sfide e prospettive", svoltosi presso il Dipartimento di Scienze Politiche dell'Università degli studi di Perugia nei giorni 16 e 17 giugno 2022[1], una specifica *call for papers* proponeva di riflettere sugli algoritmi "pubblici". La datizzazione degli elementi di realtà e l'applicazione del calcolo come meccanismo per profilare, mappare, analizzare, valutare, selezionare e prevedere/inferire costituiscono in effetti una sfida per le categorie classiche della legalità, e della legalità amministrativa, in particolare. Nella misura in cui legalità è predeterminazione, il valore (conoscitivo) aggiunto del *machine learning* – che consiste nella capacità di estrarre, esporre conoscenza inaspettata, non scontata e quindi *non prevista*, da cui trarre indicazioni e conseguenze giuridicamente rilevanti – si pone in termini ontologici come uno "scarto" rispetto al modo tradizionale di allineare sapere e regolamentazione giuridica. Può la legalità "tradizionalmente intesa" reggere a questa sfida? Cosa rischiamo di "perdere" nella crisi della legalità prodotta dall'avvento della conoscenza/regolamentazione algoritmica?

Vi è poi l'altro corno del problema. Sempre in termini oramai (tutto sommato) tradizionali, si è soliti osservare come la partecipazione abbia rappresentato il meccanismo utile a riconnettere agli interessi degli *stakeholder* l'esercizio di funzioni tecnicamente specializzate, e come tali spesso demandate ad agenzie indipendenti. Ma quale partecipazione è possibile immaginare di attivare, quando le scelte di *policy* sono elaborate sulla scorta di opzioni della cui *explainability* non si è ancora del tutto certi?

Nel corso del panel organizzato in quel convegno, la presentazione dei *paper* ha dato vita a un dibattito vivace ed approfondito, un confronto che ha anche consentito agli autori di ritornare sui rispettivi contributi, di arricchirli e di affinarli ulteriormente.

Grazie alla preziosa ospitalità della RIID, quei saggi sono oggi pubblicati in questa sezione monografica, e vogliono costituire un contributo qualificato a un dibattito autenticamente plurale, sia per gli oggetti indagati, sia per il taglio analitico proposto dai diversi autori. Come curatore (anche di quel panel), mi preme innanzitutto ringraziare tutti gli autori dei saggi per l'impegno profuso, e complimentarmi con loro per il risultato ottenuto. Sono anche grato per l'onore ed il privilegio di aver potuto collaborare a condurre in porto questo piccolo (ma denso) progetto editoriale. Infine, un ringraziamento particolare va a Marina Pietrangelo per la fiducia accordata, e a Simona Binazzi, che è davvero insostituibile, e con lei tutta l'ottima redazione della Rivista!

Perugia, 14 dicembre 2022

B. Ponti è professore associato di Diritto amministrativo presso l'Università degli studi di Perugia. Questo scritto è l'introduzione alla sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura dello stesso Autore.

[1] Programma del Convegno.

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0085
Articolo sottoposto a peer review

La sfida tecnologica alla legalità amministrativa

Alessandro Puzzanghera

Nel nuovo scenario in cui si assiste all'affermarsi della tecnologia ed in particolare allo sviluppo dell'intelligenza artificiale, ci si pone dinnanzi ad alcuni aspetti di questo imponente fenomeno e a interrogativi di tipo etico ed antropologico che rappresentano un vero e proprio cambio di paradigma, al fondo del quale potrebbe esserci una nuova idea di umanità. L'uso dei sistemi di intelligenza artificiale applicati alle attività della pubblica amministrazione impongono di riesaminare gli istituti giuridici, principi e regole dell'organizzazione e del procedimento amministrativo. In più, impongono di inquadrare correttamente la dinamica procedimentale che ne scaturisce, oltre al rapporto fra procedimento amministrativo e il principio di legalità.

Algoritmo – Decisione amministrativa – Intelligenza Artificiale – Pubblica amministrazione

Sommario: *1. Premessa – 2. Brevi cenni sul procedimento amministrativo digitalizzato – 3. Algoritmi e Intelligenza Artificiale: interviene il Consiglio di Stato – 4. Uno sguardo rivolto verso l'estero – 5. Conclusioni*

1. Premessa

Il principio di legalità costituisce un pilastro indefettibile per gli ordinamenti liberaldemocratici, specie nel quadro degli strumenti di sottoposizione del potere al sistema giuridico.

Se è indubbio che l'avvento di detto principio abbia presidiato il passaggio dallo *status subjectionis* al ruolo di *activae civitatis*, con l'arrivo dello Stato pluriclasse al contempo, già agli albori del XX secolo, Santi Romano aveva presagito l'inverarsi di un processo di crisi del modello statale i cui esiti si sono riverberati nella contemporaneità.

Attualmente, infatti, l'ordinamento generale annovera tra le criticità che lo caratterizzano, accanto alla perdita della connotazione atomistica, il proliferare di organizzazioni operanti in ambito sovranazionale, che incidono in maniera significativa sul processo di frammentazione degli interessi, interferendo altresì sui pubblici poteri nazionali. Senza poi dimenticare il ruolo assunto dal mercato e dalle sue regole che partecipa al nuovo modo di concepire i rapporti pubblico/privato.

In questo scenario si assiste all'affermarsi delle nuove tecnologie dell'informazione e della comunicazione, ivi inclusi gli algoritmi e l'Intelligenza Artificiale (IA), che potrebbero contribuire a raggiungere l'obiettivo della "buona amministrazione". Con le pronunce del Consiglio di Stato, si ammette, infatti, il ricorso ai sistemi di intelligenza artificiale nel procedimento amministrativo e vengono tracciati i principi posti a presidio dei cittadini - utenti del servizio pubblico.

A tal proposito, due sono i principi che assumono rilievo fondamentale: a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati (principio di trasparenza); b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo (principio di responsabilità).

Occorre tuttavia interrogarsi su quali potrebbero essere i meccanismi che consentano la compatibili-

A. Puzzanghera è dottorando di ricerca in "Global Studies for an Inclusive and Integrated Society. Global Culture, Digital Society, Diversity Inclusion and Social Innovation for Development" presso l'Università per stranieri "Dante Alighieri" di Reggio Calabria.
Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

tà fra l'uso di sistemi di automazione e gli istituti di garanzia di partecipazione. Pertanto, si tratta di capire quale sia il margine di applicazione dei tradizionali istituti partecipativi a fronte del ricorso all'automazione da parte dell'amministrazione.

Dinanzi all'imperante processo di innovazione, si manifesta uno stato di crisi dei fondamenti che tradizionalmente hanno connotato la riflessione dei fautori del pensiero liberale, improntato sulla garanzia della prevedibilità e stabilità delle regole, la trasparenza dei procedimenti decisionali e la responsabilità dei referenti soggettivi preposti all'esercizio delle funzioni pubbliche.

2. Brevi cenni sul procedimento amministrativo digitalizzato

Per un'analisi del fenomeno di digitalizzazione e informatizzazione amministrativa, è necessario prendere le mosse dall'esame dei vari ambiti su cui questo incide.

Come affermato a livello dottrinale[1], il primo settore che ha avvertito in maniera significativa l'influenza delle innovazioni tecnologiche e che ne ha tratto un notevole impulso è il settore dei dati, interessato da una crescita esponenziale[2]. Il trattamento di un'ampia categoria di dati raccolti, concernenti numerose persone fisiche e giuridiche, pur risultando innegabilmente vantaggioso per il perseguimento di determinati obiettivi, è potenzialmente idoneo a ledere le posizioni giuridiche soggettive di numerosi consociati.

Può anzitutto osservarsi che il progresso delle tecnologie e l'avvento di una "quarta rivoluzione industriale", orientata verso produzioni personalizzate e connotata da fattori quali l'impiego di big data, tecnologie di cloud computing, Internet delle cose, intelligenza artificiale, determinano un radicale mutamento nella dinamica dei rapporti e degli interessi in ogni ambito dell'agire umano, destinato a produrre effetti anche sulla declinazione della relazione tra libertà individuali e autorità[3] (espressione di poteri pubblici e privati)[4], sulla struttura e sull'organizzazione dello Stato e, in ultima istanza, sulla decisione amministrativa[5].

Già nel lontano 1979 Giannini aveva colto l'importanza dell'impiego delle tecnologie dell'informazione e della comunicazione da parte della pubblica amministrazione. Egli già notava che «i sistemi informativi non servono più alle amministrazioni per fatti di gestione interna ma servono proprio per amministrare, si proiettano cioè sempre più verso l'esterno»[6].

Da tempo molti paesi hanno avviato un processo di modernizzazione dei fascicoli contenuti negli archivi. Con l'introduzione di un supporto digitale per la lettura dei dati, il processo di modernizzazione ha perseguito l'obiettivo di garantire una trasmissione veloce ed agevole di informazioni tra gli uffici mediante reti interconnesse[7].

Tale innovazione costituita dall'introduzione delle reti interconnesse comporta evidenti benefici sul piano procedimentale, in quanto concede ad un ufficio la possibilità di accedere a dati detenuti da un altro ufficio o da un'altra amministrazione senza doverli richiedere ad una persona fisica e senza dover aspettare i tempi che un procedimento del genere richiederebbe. L'accesso ai dati avviene automaticamente, sulla base di una veloce procedura informatica.

Inoltre, le *Information and Communication Technologies* favoriscono anche l'accesso dei cittadini ai database della pubblica amministrazione, permettendo una maggiore trasparenza ed immediatezza nella circolazione delle informazioni anche sotto tale profilo.

La presenza di database pubblici risulta essere oggi un elemento caratterizzante delle pubbliche amministrazioni.

L'informatica non viene solo usata quale mezzo di esternazione di provvedimenti, o di atti fatti pervenire da privati all'interno di procedimenti condotti da enti pubblici: gli elaboratori si atteggiano, invece, sempre più come strumenti ai quali viene demandato l'espletamento di talune funzioni (istruttorie, ma anche decisionali), come accade nelle ipotesi di correzione automatizzata delle prove di determinati concorsi, ovvero nella gestione di procedimenti di mobilità da parte di grandi amministrazioni centrali[8].

Da un punto di vista normativo è da menzionare l'art. 3-*bis* della l. 7 agosto 1990, n. 241, ancora recentemente modificato (d.l. 16 luglio 2020, n. 76), «le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati»[9].

Inoltre, all'amministrazione digitale è stato addirittura dedicato un "codice" (d.lgs. 7 marzo 2005, n. 82, c.d. CAD) che ha lasciato emergere dei "diritti di cittadinanza digitale" (art. 17, co. 1-*quinquies*), categoria evanescente nei confini (e perciò priva di una valenza applicativa), ma che evoca la sempre più marcata rivoluzione del procedimento e del provvedimento digitalizzati.

Pertanto, dall'iniziativa, allo svolgimento dell'istruttoria (art. 41), alla partecipazione (art. 4), alla forma dell'atto (art. 20) e agli adempimenti necessari per la piena efficacia dello stesso (art. 3-*bis*), lo svolgimento della funzione amministrativa risulta profondamente inciso e conformato dalle nuove tecnologie, attraverso una disciplina legale che pare incentrata sulla dimensione organizzatoria, sul procedimento e sulla forma dell'atto[10].

La disciplina del procedimento amministrativo "tradizionale", che è esso stesso "forma sensibile della funzione"[11], è incentrata sulla possibilità per l'amministrazione di adottare la decisione sulla base di ragioni giuridiche, fatti, interessi, dei quali occorre dar conto nella motivazione dell'atto di modo che risulti – anche a garanzia del diritto di difesa – spiegabile ed individuata su basi di razionalità causale.

Il procedimento amministrativo – «sequenza di atti e operazioni che si realizzano in vista di un certo risultato di diritto amministrativo»[12] – con la sua struttura e la sua logica, nel susseguirsi di fasi successive e concatenate sino al concretarsi del potere nell'assunzione della decisione e nell'adozione dell'atto, presenta rilevanti assonanze con la strutturazione dell'algoritmo, inteso come serie finita di passaggi che permettono di risolvere un problema.

Mentre gli algoritmi trovano già spazio nell'assunzione della decisione amministrativa, il quadro normativo appare sostanzialmente invariato, lasciando emergere la necessità che l'analisi del fenomeno e l'individuazione della relativa disciplina giuridica siano condotte anzitutto sulla scorta dei principi generali e delle riflessioni di giurisprudenza e dottrina[13].

Dottrina e giurisprudenza hanno da tempo evidenziato i vantaggi che l'atto ad elaborazione elettronica presenta in termini di riduzione di rischi di disparità di trattamento, di osservanza della legge, di prevenzione di fenomeni corruttivi, di completezza dell'istruttoria.

L'ipotesi meno problematica riguarda l'atto amministrativo vincolato, la cui fattispecie è costruita secondo lo schema norma-fatto-effetto[14]; grazie a tale modello l'atto amministrativo automatizzato è entrato nell'amministrazione e, dunque, nelle riflessioni della dottrina e della giurisprudenza.

Tuttavia, la limitazione dell'impiego dell'atto amministrativo automatizzato alle sole ipotesi di attività vincolata risulta non appagante anche in ragione della stessa difficoltà di definire l'atto amministrativo vincolato e dell'ampio dibattito che anima la dottrina amministrativistica sul punto[15].

Recentemente la decisione discrezionale automatizzata inizia ad essere ammessa dalla dottrina[16] e dalla giurisprudenza e a trovare ingresso nella prassi.

Anche senza voler immaginare l'adozione di un atto amministrativo discrezionale interamente automatizzato, è evidente come già oggi gli algoritmi – ed in particolare i sistemi di IA – siano adoperati dall'amministrazione per supportarne la decisione, finendo inevitabilmente per condizionarla.

Basti pensare agli algoritmi che il Governo ha utilizzato per determinare gli scenari di rischio (c.d. "zone") e le corrispondenti misure di contenimento in relazione all'epidemia covid-19. Si tratta di un sistema che combina 21 indicatori di monitoraggio e 5 livelli di rischio[17] dando luogo a valutazioni probabilistiche che sono apparse a taluni osservatori ambigue e non trasparenti[18]. La decisione sullo scenario di rischio di ciascuna regione spettava al Ministro della Salute, ma certamente l'individuazione della tipologia di "zona" era rimessa all'algoritmo, che incideva in maniera significativa sulla scelta del decisore politico.

Davanti ad un fenomeno che cambia radicalmente i rapporti sociali, civili, politici ed economici, occorre indagare se i principi e le regole che reggono l'agire dell'amministrazione siano sufficienti a governare la complessità derivante dall'interazione continua ed esponenziale tra uomo e macchina o se, al contrario, occorra enuclearne di nuovi[19].

3. Algoritmi e Intelligenza Artificiale: interviene il Consiglio di Stato

Sebbene siano numerose le disposizioni che prevedano la digitalizzazione dei procedimenti amministrativi, vi è, tuttavia, l'assenza di una norma generale che ammetta l'impiego di sistemi di IA nell'adozione di atti amministrativi.

Tale possibilità non sembra potersi desumere da norme di carattere eminentemente programmatico (art. 3-*bis* l. n. 241/1990; artt. 12 e 41 CAD), che paiono riferite in generale all'attività amministrativa e al procedimento, ma non alla decisione o all'atto automatizzato.

Nell'incoraggiare il ricorso a forme di intelligenza artificiale nello svolgimento dell'attività amministrativa, la Sesta Sezione del Consiglio di Stato in numerose sentenze[20] ha compiuto un rinvio al principio di buon andamento dell'azione amministrativa, enunciato all'articolo 97 della Costituzione[21] e riconosciuto come uno dei valori cardine a cui la pubblica amministrazione deve ritenersi subordinata.

Nell'enunciare il principio di buon andamento, i giudici di Palazzo Spada dimostrano di ritenere che un corretto utilizzo dei nuovi strumenti digitali introdotti con la c.d. rivoluzione industriale 4.0 possa condurre ad un suo migliore rispetto.

Strettamente correlati sono i canoni di efficienza ed economicità dell'azione amministrativa, anch'essi enunciati dal Consiglio di Stato come declinazioni necessarie del principio di rango costituzionale. Entrambi i canoni trovano riconoscimento normativo all'art. 1 della legge sul procedimento amministrativo[22] ed «impongono all'amministrazione il conseguimento dei propri fini con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale»[23].

Nello specifico, i due principi valutano due aspetti leggermente diversi della performance dell'amministrazione. Il principio di efficienza comporta una comparazione tra il risultato raggiunto dalla pubblica amministrazione e le risorse disponibili, ad essere premiato è quindi un utilizzo oculato delle risorse. Diversamente, il principio di efficacia rapporta i risultati raggiunti agli obiettivi stabiliti.

Tali principi vengono condensati nel principio di economicità, anch'esso oggetto di previsione nella legge, principio che valuta l'utilizzo efficiente delle risorse amministrative e il raggiungimento in maniera efficace degli obiettivi prestabiliti.

Il Consiglio di Stato, in via teorica, ha ammesso l'atto discrezionale ad elaborazione elettronica[24], qualificando il ricorso all'algoritmo "in termini di modulo organizzativo" con una valenza meramente procedimentale ed istruttoria, rimarcando però che il procedimento amministrativo «resta il modus operandi della scelta autoritativa, da svolgersi sulla scorta della legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico, titolare del potere»[25]. Dunque, secondo i giudici di Palazzo Spada l'impiego di algoritmi da parte della pubblica amministrazione pone essenzialmente un problema di trasparenza e quindi di comprensibilità della decisione.

Sul punto, infatti, sembrano quasi sfuggenti allorquando affermano che vi sarà una difficile applicazione di alcune disposizioni della legge n. 241/1990 in un contesto digitalizzato e pertanto in una decisione automatizzata.

Da segnalare una tesi contraria avanzata da parte della giurisprudenza, fondata su una contrapposizione tra uomo e macchina quasi inconciliabile nell'adozione della decisione amministrativa.

Il T.a.r. Lazio nel 2018[26] ha ribadito il noto legame tra gli istituti posti dalla legge n. 241/1990 (quali la disciplina della motivazione, la partecipazione, la centralità del responsabile del procedimento) ed i valori costituzionali enucleati negli artt. 3, 24, 97, Cost. e nell'art. 6 della Convenzione europea dei diritti dell'uomo e ha evidenziato le difficoltà che l'interprete incontra quando vuole applicare detti principi e regole alle decisioni automatizzate.

Invero, il Collegio è del parere che le procedure informatiche, anche ove raggiungano addirittura la perfezione, non potranno mai sostituire appieno l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere, il quale, è in grado di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento.

Come scritto precedentemente, nel ricorrere all'algoritmo come scelta organizzativa dell'ente si è sempre fatto riferimento agli algoritmi impiegati nell'adozione di atti amministrativi vincolati, in un contesto in cui si negava l'ammissibilità dei provvedimenti automatizzati a carattere discrezionale.

L'impiego di algoritmi "non deterministici" nell'adozione del provvedimento automatizzato o della decisione comporta un radicale mutamento nel processo di formazione della volontà espressa attraverso l'atto, tale da incidere su ineludibili garanzie e diritti intorno ai quali è stato costruito l'ordinamento amministrativo.

Tali garanzie vengono messe in discussione dall'orientamento secondo il quale, da un lato, non si può escludere l'uso di algoritmi anche nell'ambito dell'attività discrezionale, dall'altro, il ricorso all'algoritmo a supporto della decisione amministrativa è espressione della potestà auto-organizzatoria e, dunque, non vi è la necessità di una norma di legge *ad hoc*.

Per citare Picozza, si è arrivati alla "fine di un'era" e pertanto i tempi sono maturi per una riflessione ampia sui principi e sulle regole generali che dovrebbero presiedere all'uso di sistemi di IA nella decisione amministrativa, riducendo in questo modo le difficoltà che derivano dall'applicazione di regole esistenti che si rivelano essere talvolta inadeguate oltre all'assenza di presidi di legalità idonei a garantire diritti ed interessi nel mutato rapporto tra libertà ed autorità.

Si correrà il rischio di ritrovarsi affidati a sistemisti e progettisti di software, anche estranei all'ente, i quali sono chiamati a ricoprire un ruolo rilevante nell'organizzazione amministrativa e nell'azione amministrativa.

Ne deriva che sia strettamente necessaria la presenza di un sistema normativo primario, per l'applicazione dell'IA nell'adozione di decisioni amministrative, che preveda la possibilità di delega del potere decisionale alla macchina (legalità formale), ma anche i principi che devono disciplinare l'esercizio di tale delega (legalità sostanziale).

4. Uno sguardo rivolto verso l'estero

Facendo leva sulle considerazioni fatte nel presente scritto emerge una forte pressione da parte dell'Unione europea nei confronti degli Stati membri.

L'Unione europea ha dettato una linea: l'intelligenza artificiale deve essere uno strumento per il raggiungimento del benessere dell'individuo e della società nel suo insieme.

Il 21 aprile 2021 la Commissione europea ha presentato la tanto attesa proposta di regolamento che stabilisce norme armonizzate in materia di IA.

La *Proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale* (*legge sull'intelligenza artificiale*)[27] ha l'obiettivo di armonizzare la legislazione europea sull'IA, facendo leva sull'innovazione, la sicurezza e la tutela dei diritti individuali. In anticipo sulla proposta della Commissione sull'IA, il Parlamento aveva costituito un gruppo specializzato per analizzare l'impatto dell'IA sull'economia dell'Unione europea.

La crisi pandemica, inoltre, ha rappresentato una spinta ad un mercato molto più "on-line" oltre che la possibilità di avere risorse finanziarie senza precedenti per portare a termine alcuni processi di trasformazione, tra cui la transizione digitale.

La digitalizzazione amministrativa potrebbe portare a formule tecniche, precise e omogenee, costringendo alla redazione di istruzioni semplice e chiare, che comporterebbero una riduzione dei dubbi interpretativi e andrebbero a formare una guida semplice per la soluzione delle eventuali antinomie normative[28] e un tale sviluppo potrebbe comportare un miglioramento legislativo in generale, soprattutto se il principio di legalità venisse interpretato come esigenza di una ampia disciplina di rango primario.

Tuttavia, si potrebbe correre il rischio di un irrigidimento oltre ad un impoverimento della normazione, in proposito, alcuni studiosi hanno parlato di "neopositivismo digitale", ovvero una sopravvalutazione delle istruzioni normative e, pertanto, una mancanza di interpretazione, trasformando il computer come bocca della legge[29].

In Spagna la legge definisce l'attività amministrativa automatizzata come attività prodotta attraverso un sistema informatico opportunamente programmato senza necessità di intervento di una persona fisica per ogni singolo caso e dispone che in caso di attività amministrativa automatizzata, è necessario indicare l'organo competente per la definizione di specifiche, la programmazione, il mantenimento, la supervisione ed il controllo di qualità e, eventualmente, la revisione del sistema informatico e del suo codice sorgente.

In Francia il *Code des relations entre le public et l'administration* fornisce una base legale all'impiego di sistemi di IA da parte dell'ente: ai sensi dell'art. L.311-3-1 (introdotto nel 2016) l'amministrazione che adotta un atto sulla base di un algoritmo deve informare l'interessato e deve fornire indicazioni sul trattamento dei dati. Più nel dettaglio l'amministrazione è tenuta a fornire maggiori informazioni, con riguardo ai dati trattati, le loro fonti, i parametri di trattamento, la loro ponderazione e le modalità dell'elaborazione algoritmica. Le amministrazioni devono pubblicare le regole che sovraintendono all'utilizzo di questi strumenti.

In Germania nel 2016 è stata introdotta nella legge sul procedimento amministrativo (VwVfG) una nuova disposizione (art. 35.a) che ammette l'atto vincolato interamente automatizzato a condizione che sussista una specifica base legale.

Il Regolamento UE 679/2016 (c.d. GDPR), infatti, 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» (art. 22).

Il divieto di decisione (privata e pubblica) «basata unicamente sul trattamento automatizzato di dati» non si applica quando essa «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» (art. 22, § 2, lett. b).

Ai sensi dell'art. 23 GDPR, l'ordinamento nazionale o dell'Unione può limitare attraverso misure legislative, il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato a condizione che tale limitazione «rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica» per garantire la tutela degli interessi pubblici.

Il GDPR ammette il ricorso a una decisione basata unicamente sul trattamento automatizzato di dati personali in presenza di una norma che, nel rispetto del principio di proporzionalità, deve indicare «misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

In presenza di un sistema tecnico in forza del quale, nel rapporto uomo-macchina, il potere decisionale è integralmente affidato alla seconda, l'ordinamento europeo avverte la necessità che sia garantito attraverso la legge il diritto ad una buona amministrazione nella sua opera di digitalizzazione.

I principi costituzionali (artt. 3, 24 e 113, 97) ed il diritto europeo (art. 41 Carta dei diritti fondamentali dell'UE) prevedono che debba essere la legge ad ammettere la scelta dell'Amministrazione di adottare atti amministrativi che, pur se non integralmente automatizzati, implichino comunque l'impiego di un sistema di IA.

5. Conclusioni

Si ritiene che la legge non dovrebbe limitarsi ad attribuire alle amministrazioni il potere di ricorrere all'uso delle nuove tecnologie per adottare provvedimenti che già rientrano nella loro sfera di competenza, ma dovrebbe anche specificare i principi e le regole che devono essere osservate nella definizione, progettazione e implementazione del sistema che conduce all'adozione

della decisione automatizzata e che potrebbero essere adeguate alla peculiarità dei singoli procedimenti anche attraverso norme di rango secondario.

L'assenza di una normativa specifica sul tema, pronta ad accogliere l'innovazione e a disciplinarla nella maniera più proficua per permetterle di svolgere il suo compito, ha provocato oscillazioni giurisprudenziali e un'iniziale incertezza nell'applicazione di tali strumenti.

Pertanto, servirebbe una disposizione che consentisse la partecipazione dei soggetti potenzialmente interessati al processo di definizione dell'algoritmo e di scrittura del codice sorgente.

Si dovrebbero prevedere in via obbligatoria un periodo di preventiva sperimentazione dell'efficacia del sistema nonché adeguati procedimenti di auditing, analisi d'impatto e monitoraggio *ex post* del funzionamento dell'algoritmo.

Non meno importante è l'osservanza – sin dall'impostazione dell'algoritmo – del principio di "conoscibilità" e di "comprensibilità" dei processi decisionali automatizzati che riguardano il cittadino, al quale deve essere riconosciuto in ogni caso il diritto di ricevere informazioni significative sulla logica utilizzata, sulla selezione degli scenari, sui casi di studio utilizzati per validare il sistema e sul metodo di addestramento dell'algoritmo.

Di fronte a forme di opacità intrinseche all'algoritmo, spesso diviene difficile garantire la conoscibilità di tutti gli aspetti caratterizzanti la decisione elaborata elettronicamente.

Vi è poi il principio di "non discriminazione algoritmica" in forza del quale l'algoritmo deve essere costruito a monte, e rettificabile successivamente, in modo da garantire che la profilazione non produca effetti discriminatori sulla base dell'origine etnica, del genere, delle opinioni politiche, religiose o personali, dell'orientamento sessuale.

Qualora, infatti, l'algoritmo fosse costruito o addestrato su un set di dati discriminatorio, le relative decisioni sarebbero "intrinsecamente" illegittime.

Il responsabile del procedimento potrebbe pervenire alla decisione e adottare il provvedimento, trovando nell'apporto partecipativo degli interessati argomenti persuasivi di carattere tecnico e giuridico che eventualmente lo inducano a discostarsi dalla proposta dell'elaboratore.

In forza del "principio di non esclusività della decisione algoritmica", nel processo decisionale dovrebbe esistere comunque un contributo umano capace di controllare, validare o smentire la decisione automatica.

In conclusione, si evidenzia che nel percorso verso l'impiego dei sistemi di IA da parte dell'amministrazione occorre dunque superare le prospettive di radicale ed inconciliabile contrapposizione tra uomo e macchina, avvalendosi, però, della garanzia della legalità amministrativa che costituisca il riferimento verso un progresso che sia non solo tecnologico, ma anche di tutela dei diritti e delle libertà individuali.

Note

[1]Sul tema, si segnala J.B. Auby, *Il diritto amministrativo di fronte alle sfide digitali*, in "Istituzioni del federalismo", 2019, n. 3.

[2]Il tema viene trattato nell'indagine conoscitiva sui big data, realizzata congiuntamente dall'Autorità per le garanzie nelle comunicazioni (AGCOM), dall'Autorità garante della concorrenza e del mercato (AGCM) e dal Garante per la protezione dei dati personali. L'indagine viene avviata rispettivamente con delibera AGCOM n. 217/17/CONS, con provvedimento AGCM del 30 maggio 2017, n. 26620, e dal Garante sulla base delle determinazioni dell'adunanza collegiale dell'11 maggio 2017. Come si evince dall'indagine, l'incremento nell'utilizzo di dati ha raggiunto livelli esponenziali. Nell'anno 2018, si è registrato un volume totale di dati di 28 *zetabyte* (ZB), che costituisce un aumento di più di dieci volte rispetto ai dati registrati nel 2011.

[3]L'inversione di prospettiva nell'analisi del rapporto tra autorità e libertà si deve anche alle riflessioni di V. Caputi Jamberenghi, *Uffici ed impiegati pubblici dallo Statuto albertino alla Costituzione nei centocinquant'anni di Unità d'Italia (veduta di scorcio)*, in "Giustamm.it", 2011, n. 12. Secondo A. Angiuli, V. Caputi Jamberenghi, *A proposito di gradualismo e superamento delle dicotomie: una metafora e un binomio da invertire*, in "Il diritto dell'economia", 2019, n. 3, p. 22, «se ad una dicotomia è necessario ricorrere, quella più conforme all'ordinamento derivato di diritto amministrativo è libertà-autorità; laddove il primo termine riecheggia l'origine del potere amministrativo, l'origine dell'autorità [...]. È, in realtà, soltanto da un fatto di esercizio di libertà che può sorgere ed essere successivamente accolto il provvedimento dell'autorità, il suo intervento nettamente orientato e rivolto verso una realizzazione conforme al principio di libertà».

[4]A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.-U. Galetta (a cura di), "Il diritto dell'amministrazione pubblica digitale", Giappichelli, 2020, p. 2 ss.

[5]Per queste considerazioni, cfr. P. Otranto, *Decisione amministrativa e digitalizzazione della P.A.*, in "federalismi.it", 2018, n. 2. Sull'"Amministrazione 4.0", cfr. anche D.-U. Galetta, J.G. Corvalan, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in "federalismi.it", 2019, n. 3.

[6]M.S. Giannini, *Rapporto sui principali problemi dell'amministrazione dello Stato*, in "Il Foro italiano", 1979, V, c. 289 ss.

[7]In G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018, le reti interconnesse vengono definite come «sistema informatico nel quale due o più unità funzionali sono in grado di comunicare e quindi scambiare informazioni tra loro in modo automatizzato, consentendo così l'accesso a dati conservati su un sistema diverso da quello richiedente le informazioni stesse».

[8]A.G. Orofino, *L'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi*, in "Giornale di diritto amministrativo", 2004, n. 12, p. 1371.

[9]D.-U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni anche alla luce degli ultimissi-*

mi arresti in materia, in "Rivista italiana di diritto pubblico comunitario", 2020, n. 3-4, p. 505.

[10]E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2, pp. 277-281.

[11]F. Benvenuti, *Funzione amministrativa, procedimento, processo*, in "Rivista trimestrale di diritto pubblico", 1952, n. 1, p. 129.

[12]A.M. Sandulli, *Manuale di diritto amministrativo*, X ed., Jovene, 1969, p. 373.

[13]P. Forte, *Diritto amministrativo e* data science. *Appunti di intelligenza amministrativa artificiale (AAI)*, in "P.A. Persona e Amministrazione", 2020, n. 1, p. 254 ss.

[14]E. Capaccioli, *Manuale di diritto amministrativo*, Cedam, 1983, p. 267 ss. In dottrina si registra un consenso pressoché unanime sull'ammissibilità dell'atto automatizzato vincolato a partire dagli studi di G. Duni, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto emanato nella forma elettronica*, in "Rivista amministrativa della Repubblica italiana", 1978, p. 407 ss.

[15]In ordine al rapporto tra vincolatezza ed atto automatizzato, cfr. L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in "Il Foro Amministrativo", 2018, n. 9, p. 1619 ss.

[16]Su questi temi, cfr. le osservazioni di R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in "Diritto amministrativo", 2020, n. 2, p. 305 ss.

[17]La struttura dell'algoritmo e gli indicatori di riferimento sono previsti dal decreto 30 aprile 2020 del Ministro della Salute. Sul punto si vedano le notazioni di C. Acocella, *Ancora su diritto e tecnica. Le valutazioni tecnico-scientifiche come premessa delle decisioni politico-amministrative assunte per fronteggiare l'emergenza pandemica da covid-19*, in "P.A. Persona e Amministrazione", 2020, n. 2, p. 287 ss.

[18]F. Fuga, *Colori delle Regioni, non fidiamoci dell'algoritmo: ecco perché*, in "agendadigitale.eu", 20 novembre 2020.

[19]I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in "Istituzioni del federalismo", 2019, n. 3, p. 643 ss.

[20]Si richiamano le seguenti pronunce: Consiglio di Stato, Sez. VI, sentenza del 4 febbraio 2020, n. 881; Consiglio di Stato, Sez. VI, sentenze del 13 dicembre 2019, n. 8472-8473-8474; Consiglio di Stato, Sez. VI, sentenza 8 aprile 2019, n. 2270.

[21]«I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione». Art. 97 Cost.

[22]«L'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di imparzialità, di pubblicità e di trasparenza, secondo le modalità previste dalla presente legge e dalle altre disposizioni che disciplinano singoli procedimenti, nonché dai princìpi dell'ordinamento comunitario». Art. 1, l. 241/1990.

[23]Consiglio di Stato, Sez. VI, sentenza del 4 febbraio 2020, n. 881; Consiglio di Stato, Sez. VI, sentenze del 13 dicembre 2019, n. 8472-8473-8474; Consiglio di Stato, Sez. VI, sentenza 8 aprile 2019, n. 2270.

[24]Consiglio di Stato, n. 8472/2019, cit., § 11: «Né vi sono ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse. In disparte la stessa sostenibilità a monte dell'attualità di una tale distinzione, atteso che ogni attività autoritativa comporta una fase quantomeno di accertamento e di verifica della scelta ai fini attribuiti dalla legge, se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini predetti, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità. Piuttosto, se nel caso dell'attività vincolata ben più rilevante, sia in termini quantitativi che qualitativi, potrà essere il ricorso a strumenti di automazione della raccolta e valutazione dei dati, anche l'esercizio di attività discrezionale, in specie tecnica, può in astratto beneficiare delle efficienze e, più in generale, dei vantaggi offerti dagli strumenti stessi».

[25]Consiglio di Stato, n. 8472/2019, cit., §10; *id.*, sez. VI, 4 febbraio 2020, n. 881.

[26]T.a.r. Lazio - Roma, sez. III-*bis*, 10 settembre 2018, n. 9224-9230.

[27]Doc. COM(2021) 206 del 21 aprile 2021.

[28]L. Reisinger, *Sistemi normativi e tavole di decisione*, in "Informatica e diritto", 1979, n. 1, p. 139 ss.

[29]E. Schmidt-Aßmann, A-K. Kaufhold, *Der Verfahrensgedanke im deutschen und europäischen Verwaltungsrecht*, in M. Eifert, C. Möllers, A. Voßkuhle (hrsg.), "Grundlagen des Verwaltungsrechts", III ed., vol. II, 2022, ann. marg. p. 83.

* * *

The technological challenge to administrative legality

Abstract: In the new scenario in which we are witnessing the affirmation of technology and in particular to the development of artificial intelligence, we are faced with some aspects of this impressive phenomenon and ethical and anthropological questions that represent a real paradigm shift, at the bottom of which there could be a new idea of humanity. The use of artificial intelligence systems applied to the activities of the Public Administration requires that the legal institutions, principles and rules of the organization and of the administrative procedure are re-examined. In addition, they require that the resulting procedural dynamics are correctly framed, as well as the relationship between the administrative procedure and the principle of legality.

Keywords: Administrative decision – Algorithm – Artificial Intelligence - Public Administration

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0092
Articolo sottoposto a peer review

Efficient and trustworthy decision making through human-in-the-loop visual analytics: A case study on tax risk assessment

Walter Didimo • Luca Grilli • Giuseppe Liotta • Fabrizio Montecchiani

Data mining and AI techniques are increasingly being used to automate data analysis. Ideally, one may wish to completely automate the data analysis process, but in many real-world applications a full automation may pose significant risks. In these cases, human analysts must be directly involved to refine the analysis or to make the final decisions. A challenging problem, therefore, is how to perform efficient and trustworthy decision-making when humans are an integral part of the analysis pipeline. We propose a "human-in-the-loop" methodology that leverages data mining, machine learning, and visual analytics to improve and speed up the analysis. A key feature is the use of a dashboard that integrates intuitive visual tools, which aid analysts to efficiently discover hidden data patterns or to get helpful insights. We describe in particular how this methodology has been successfully applied to support Revenue Agency officers in tax risk assessment.

Human-in-the-loop – Visual analytics – Data mining – Tax risk assessment

Summary: *1. Introduction – 2. Human-in-the-loop methodology for data analysis – 3. Case study: tax risk assessment – 3.1. Suspicious pattern definition – 3.2. Suspicious pattern matching – 3.3. Automatic preliminary taxpayers' risk assessment – 3.4. Visual exploration of matching results – 4. Final remarks*

1. Introduction

In a digitized world, the extraction of knowledge from data is a fundamental need to support decisions or predict the behavior of observed phenomena. Advances in data mining, machine learning and AI play a critical role in optimizing this process, and potentially might completely automate it, including the decision-making phase. Figure 1 shows an illustration of a fully automated data analysis. Data from various sources are collected and stored based on appropriate data models. Specific data portions, in a predefined format, are then automatically extracted and passed to the data processing phase, whose outcome is a prediction or a decision that triggers some action. No human is involved in this analysis pipeline, apart from its design, configuration and periodic supervision. Today, there are several software applications or features that work this way. For example, anti-spam filters automatically classify an incoming email as spam, and move it to the junk folder, without a direct interaction with the user.

Attempts to completely automate data-driven decision-making are being made in several fields such as finance, e-commerce, health, automotive, cybersecurity and the environment. For instance, many cybersecurity companies are investing a lot of resources to develop security incident response automation[1]. They wish to provide systems that can respond to cyberattacks at computer speeds – with a very limited human involvement – by exploiting machine learning and AI techniques.

The Authors belong to the Department of Engineering, University of Perugia. This work was supported in part by the University of Perugia, Fondi di Ricerca di Ateneo 2021, Project "AIDMIX—Artificial Intelligence for Decision Making: Methods for Interpretability and eXplainability". This essay is part of the special section on *Gli algoritmi pubblici tra legalità e partecipazione* edited by Benedetto Ponti.

However, at least in the short term, a full automation may pose significant or unacceptable risks, in many application domains. Apart from (possible) ethical problems, the main issue is about the level of uncertainty that often characterizes the data in input to the processing phase, which, in turn, propagates to its outcome. In other words, the uncertainty may drastically compromise the accuracy of automated analysis. It is also unclear how machine learning algorithms may react to inputs that significantly differ from those used in the training phase. Because of this uncertainty, an AI-based software that automates clinical diagnoses can pose serious risks to patients' health and safety, if no rigorous human validation of its outcomes is carried out. In these cases, the data analysis process must necessarily include the presence of a human analyst, who is the responsible for making the final decisions or for refining the analysis[2].

There exists an extensive body of literature devoted to describe the role that humans play in the development of effective machine learning algorithms, which is referred to as *human-in-the-loop machine learning* (*HILML*)[3].

More in general, human-in-the-loop approaches are not only restricted to machine learning, but they are attracting increasing interest in data science. Here, the idea is to make humans an integral part of the data analysis pipeline, since some tasks may require the sensitivity of a human analyst with high experience in the specific application domain. This emerging topic, known as *human-in-the-loop data analysis* (*HILDA*)[4], focuses on how to optimize the human-computer cooperation through the usage of suitable user interfaces and interaction models. In particular, when using ML or AI engines in data analysis systems, human analysts may strongly benefit from visual analytics techniques to understand the decisions or predictions made by these engines[5].

Information visualization tools are therefore key components in the fields of HILDA and explainable AI, since they provide a valuable aid in the design of decision support systems based on the human-in-the-loop paradigm. According to this paradigm, the user constantly interacts with the system with the aim to: (*i*) convey to the system their knowledge and experience in order to provide rules or tuning mechanisms for the machine learning engines; (*ii*) inspect the results automatically provided by the system in order to understand the nature of such results and validate their appropriateness, reliability, and usability, depending on the specific domain of interest.

Hereafter, we propose a human-in-the-loop methodology that leverages visual analytics techniques to improve and speed up the data analysis process. The methodology stems from the experience gained in the development of three decision support systems for tax risk assessment, whose effectiveness has been experimentally validated in previous works[6].

2. Human-in-the-loop methodology for data analysis

Our human-in-the-loop methodology is illustrated in Figure 2 and relies on the following principles:

- *final human validation*: final decisions are always made by a human analyst, machine learning and AI modules can be used, but the analysis cannot be completely automated, and a human mediation is mandatory;
- *human-centered analysis*: the analyst plays a central role in the data analysis process, providing valuable knowledge and expertise, in particular, they interact with the system throughout the process by:
  (i) selecting the data sources;
  (ii) defining the analysis entry point;
  (iii) choosing the data processing algorithms;
  (iv) exploring the results of the system;
  (v) validating and refining the results.
- *visual analytics-driven workflow*: the analyst interacts with a UI dashboard, in a domain-specific software system, to carry out every analysis task; the dashboard integrates sophisticated visualization techniques and visual tools to speed up the analysis, to discover hidden data patterns or to get helpful insights.

The proposed methodology gives a very abstract outline of how the analysis process should be conducted. In particular, the goals and the specific analysis tasks, as well as the type of data itself may drastically impact on the UI, on the visual analytics techniques, on the data model, and on the processing algorithms. Therefore, for a more concrete understanding, we will describe a case study of our methodology to support Revenue Agency officers in the tax risk assessment[7].

3. Case study: tax risk assessment

Revenue Agency (RA) officers devote a lot of work to discover tax evasion and tax avoidance. The *fiscal audit process* refers to the set of activities they carry out for this purpose. This process largely consists of the analysis of data within the RA database, which includes information about single taxpayers and their relationships like *economic transactions*, *shareholdings*, and *corporate positions*. Specifically, analysts look for certain interactions among taxpay-

ers, called *suspicious patterns*, that could reveal tax evasion activities. Suspicious patterns are derived by abstracting the characteristic traits of real cases of tax evasion/avoidance or, more in general, of fiscal risky schemes. They can be conveniently modeled as topological structures, i.e. as small groups of interconnected entities, along with the specification of some constraints on economic attributes associated with these entities and/or with their interconnections. For example, Figure 3a shows a real case of a risky scheme involving a company (C1) in the building sector and a real estate company (C2). C1 sells a building to C2, issues an invoice for 1 million euro, declares its VAT debt for this invoice, but never pays it. While C2 requests a refund for the VAT credit of its purchase. By analyzing the refund request, RA officers discovered that C1 and C2 were owned by the same taxpayer (T1). The VAT refund was therefore denied by the RA, due to the high fiscal risk exhibited by this scheme. A specific suspicious pattern, named SuppliesFromAssociated, has been derived from this real case of risky scheme (see Figure 3b for an illustration). This pattern has a triangular topology, where both the seller (C1) and the buyer (C2) of an economic transaction are participated by the same subject (T1). To generalize the pattern, the following additional rules have been included: the amount of the economic transaction is greater than or equal to a specified threshold Y; the VAT payment of the seller is less than a specified threshold Z; the VAT credit declared by the buyer is higher than a specified threshold X.

Since suspicious patterns have an inherent topological structure, their detection can be significantly improved by adopting a *taxpayer network* data model, which can be built from the RA (relational) database and stored into a graph database[8]. In a *taxpayer network* $\mathcal{N}$, each node ν of $\mathcal{N}$ represents a single taxpayer, i.e. either an individual or a legal person, like a private company or a public institution. Whereas arcs in $\mathcal{N}$ are directed and model economic relationships between pairs of taxpayers. For example, an arc (μ, ν) may represent an economic transaction where taxpayer μ is the seller and taxpayer ν is the buyer.

Ideally, a fully automated fiscal audit could work as follows. Let E be the total set of actual tax evasion attempts or events that can be revealed by an optimal analysis of the taxpayer network.

- A first set $C \supset E$ of candidate risky schemes is automatically extracted from $\mathcal{N}$.
- Then, every element in $C \setminus E$ is (automatically) filtered out by performing a suitable data processing on the input C.
- Eventually, the final output is an automated generated report describing each element of E.

Unfortunately, due to various sources of uncertainty, the aforementioned automated analysis fails, namely it may produce many false positives and false negatives. The main sources of uncertainty are listed below.

- *Missing or imprecise data sources*: a taxpayer network typically contains several hundred thousand nodes and some million arcs, consequently some data items could be missing, wrong, imprecise, or outdated.
- *Inherent uncertainty of risky schemes*: the identification of risky schemes necessarily requires an implicit or explicit knowledge of their models (i.e., suspicious patterns), but every model is an approximation of the real world.
- *High dimensionality of* $\mathcal{N}$: there are various kind of nodes and arcs in $\mathcal{N}$, which may have several attributes of different types, therefore the identification of reliable models of risky schemes may require an infeasible number of observations.
- *Unpredictability of future risky schemes*: future risky schemes can be substantially different from those already known, but detection strategies are based on the latter ones.

We therefore propose a human-in-the-loop methodology for discovering actual risky schemes in a taxpayer network. Our methodology focus on how to support human analysts – through a suitable visual analytics system – to efficiently find a set E' of risky schemes such that E' is hopefully a good approximation of E. The final decision about whether a specific risky scheme in E' is an actual tax evasion activity can be made only by human analysts after a rigorous examination of the related documentation; we omit the description of this phase because it does not involve any digital tool. Set E' can be found through several analysis loops that require a strong user involvement. Salient steps of a generic iteration are listed below:

- Suspicious pattern definition
- Suspicious pattern matching
- Automatic preliminary taxpayers' risk assessment
- Visual exploration of matching results.

We now briefly describe each of them in a separated subsection.

3.1. Suspicious pattern definition

Due to the enormous size of a typical taxpayer network, it is not possible to explore it as a whole. Indeed, risky schemes of E' can be found by exploring only small subnetworks $\mathcal{S}_i$ $(1 \leq i \leq |E'|)$ of $\mathcal{N}$ containing taxpayers' interactions that conform to some suspicious pattern. The specification of a suspicious pattern is therefore the entry point for the extrac-

tion of these subnetworks of $\mathcal{N}$. Analysts, based on their domain knowledge, can define new suspicious patterns using a high level domain-specific visual language (see, e.g., Figure 4)[9], which significantly speeds up this step. Moreover, a library of known suspicious patterns can be easily created and reused.

3.2. Suspicious pattern matching

Let $E'(P) \subset E'$ be the set of risky schemes associated with a specific suspicious pattern P. The extraction of the corresponding subnetworks $\mathcal{S}_j$ $(1 \leq j \leq |E'(P)|)$ is carried out by running a graph pattern matching algorithm on the whole taxpayer network (see Figure 5 for an illustration). Basically, this algorithm takes in input P and $\mathcal{N}$, and returns all the subnetworks in $\mathcal{N}$ that match P. The use of a graph database to store the taxpayer network makes it possible to efficiently identify subnetworks S_j.

3.3. Automatic preliminary taxpayers' risk assessment

Analysts have to assess the fiscal risk of taxpayers in the subnetworks returned by the previous matching algorithm. This phase can be partially automated by assigning to each taxpayer certain risk indexes, which provide a first estimation of their fiscal risk. Furthermore, risk indexes make it possible to rank taxpayers from the most risky to the least risky. Analysts can therefore start their in-depth investigations from the riskiest ones. Various types of risk indexes are computed, including both classical social network analysis (SNA) indexes and some domain-specific indexes. We also make use of a tax risk forecasting model[10] based on machine learning algorithms. The forecasting model is trained on the basis of the outcome of previous fiscal audits. It turns out to be quite effective on identifying the most risky taxpayers. Furthermore, based on the consensus that risky subjects may negatively affect the behavior of their business partners, we apply an information diffusion method to propagate the fiscal risk in the taxpayer network. The diffusion process is based on a stochastic model that simulates the spread of an information over an underlying network.

3.4. Visual exploration of matching results

Starting from the subnetworks returned by the graph pattern matching phase, analysts carry out a visual exploration of its neighborhood in the taxpayer network, enriched with the fiscal risk scores (see, e.g., Figure 6)[11].

The purpose of this phase is to support the analyst in validating the fiscal risk scores assigned by the previous phase. This human validation activity is fundamental for the tax administration, which must have complete control over the taxpayer selection process. In fact, thanks to a visual exploration of the taxpayer network, the analyst can better assess the real risk profile of taxpayers, thus carrying out a more effective selection of tax audits. Namely, the analyst can find new risky graph patterns or false negative cases. This information closes the loop of the system by enriching the pattern library and by improving the performance of the forecasting model.

4. Final remarks

We have described a human-in-the-loop methodology to support an efficient and trustworthy decision-making process. As clearly emerged in the description of the tax risk assessment case study, an effective application of this methodology requires a strong involvement of domain experts, whose contribution embraces both the usage of decision support systems and the design and tuning of their software modules.

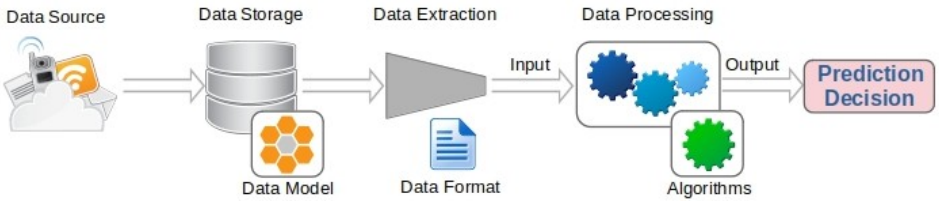


Figure 1: Illustration of a fully automated data analysis

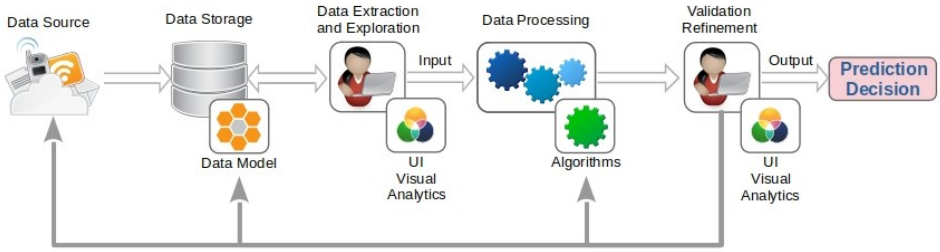
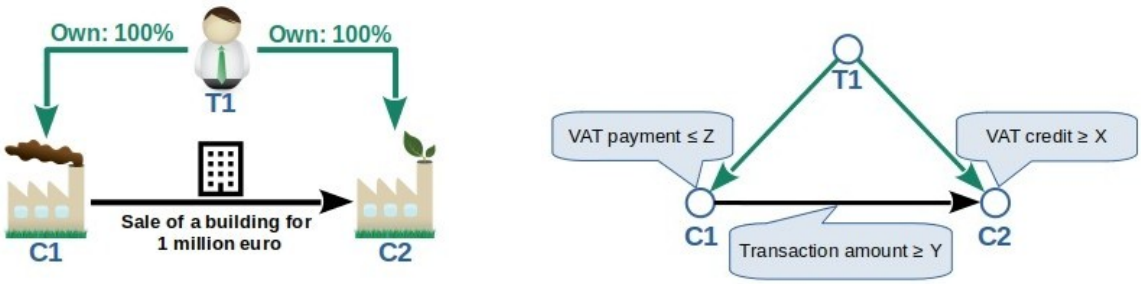


Figure 2: Illustration of a human-in-the-loop methodology for data analysis



(a) real case of a risky scheme

(b) suspicious pattern SuppliesFromAssociated

Figure 3: Illustration of (a) real case of a risky scheme and of (b) the corresponding suspicious pattern

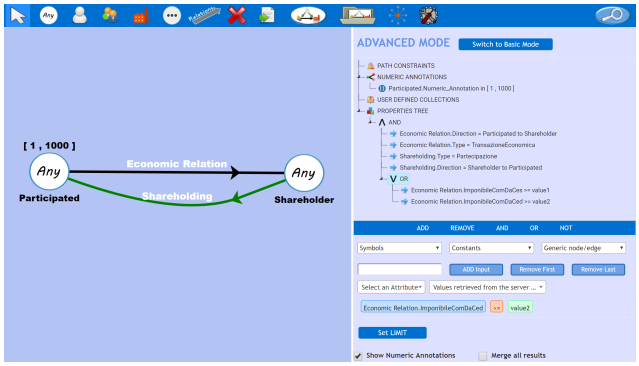


Figure 4: Graphical interface used in TaxNet to define a suspicious pattern

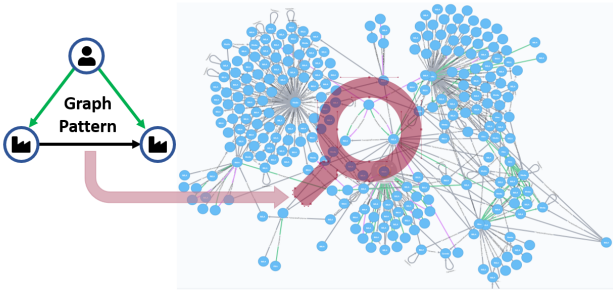


Figure 5: Tax officers encode risky relational schemes among taxpayers into suspicious graph patterns to be searched in the taxpayer network. The pattern in the figure represents a SuppliesFromAssociated scheme, consisting of an economic transaction (black edge) and two shareholding relationships (green edges)

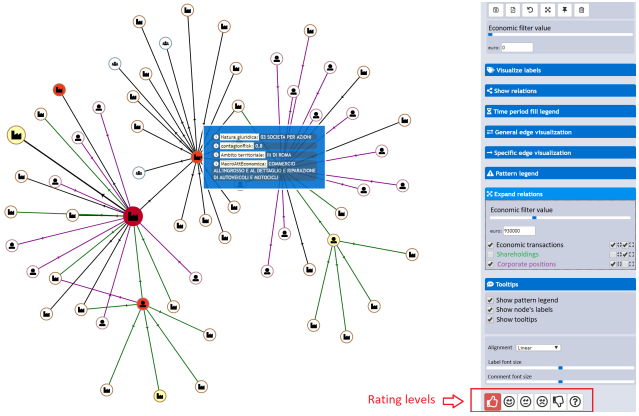


Figure 6: Visualization of a portion of the taxpayer network in MALDIVE Starting from a *high-risk* subject (dark red background), the analyst expands the network by exploding the relationships of some taxpayers. Black edges represent economic transactions, green edges are shareholdings, and purple edges are corporate positions. At the end of the analysis the analyst may add a personal feedback to the record of the investigated taxpayers

Note

[1] C. Lawson, *Market Guide for Security Orchestration, Automation and Response Solutions*, Gartner, 2022.

[2] S. Budd, E.C. Robinson, B. Kainz, *A survey on active learning and human-in-the-loop deep learning for medical image analysis*, in "Medical Image Analysis", vol. 71, 2021, 16 p.

[3] *Ibidem*; R.M. Monarch, *Human-in-the-Loop Machine Learning: Active learning and annotation for human-centered AI*, Manning, 2021; E. Mosqueira-Rey, E. Hernández-Pereira, D. Alonso-Ríos et al., *Human-in-the-loop machine learning: a state of the art*, in "Artificial Intelligence Review", 17 August 2022; X. Wu, L. Xiao, Y. Sun et al., *A survey of human-in-the-loop for machine learning*, in "Future Generation Computer Systems", vol. 135, 2022, pp. 364-381.

[4] A. Doan, *Human-in-the-Loop Data Analysis: A Personal Perspective*, in "Proceedings of the Workshop on Human-In-the-Loop Data Analytics", Association for Computing Machinery, 2018, pp. 1-6.

[5] F. Cheng, Y. Ming, H. Qu, *DECE: Decision Explorer with Counterfactual Explanations for Machine Learning Models*, in "IEEE Transactions on Visualization and Computer Graphics", vol. 27, 2021, n. 2, pp. 1438-1447; J. Choo, S. Liu, *Visual Analytics for Explainable Deep Learning*, in "IEEE Computer Graphics and Applications", vol. 38, 2018, n. 4, pp. 1558-1756; Z. Jin, Y. Wang, Q. Wang et al., *GNNLens: A Visual Analytics Approach for Prediction Error Diagnosis of Graph Neural Networks*, in "IEEE Transactions on Visualization and Computer Graphics", 4 February 2022; H. Li, M. Xu, Y. Wang et al., *A Visual Analytics Approach to Facilitate the Proctoring of Online Exams*, in P. Bjørn, S. Drucker (eds.), "Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems", Association for Computing Machinery, 2021; J. Yuan, C. Chen, W. Yang et al., *A survey of visual analytics techniques for machine learning*, in "Computational Visual Media", vol. 7, 2021, pp. 3-36.

[6] W. Didimo, L. Giamminonni, G. Liotta et al., *A visual analytics system to support tax evasion discovery*, in "Decision Support Systems", vol. 110, 2018, pp. 71-83; W. Didimo, L. Grilli, G. Liotta et al., *Combining Network Visualization and Data Mining for Tax Risk Assessment*, in "IEEE Access", vol. 8, 2020, pp. 16073-16086; Id., *Visual querying and analysis of temporal fiscal networks*, in "Information Sciences", vol. 505, 2019, pp. 406-421.

[7] Further details can be found in: W. Didimo, L. Giamminonni, G. Liotta et al., *A visual analytics system*, cit.; W. Didimo, L. Grilli, G. Liotta et al., *Combining Network Visualization*, cit.; Id., *Visual querying*, cit.

[8] E.g., Neo4j.

[9] W. Didimo, L. Giamminonni, G. Liotta et al., *A visual analytics system*, cit.

[10] W. Didimo, L. Grilli, G. Liotta et al., *Combining Network Visualization*, cit.

[11] *Ibidem*.

* * *

Processi decisionali efficienti e affidabili tramite analisi visuale con metodologia *human-in-the-loop*: un caso di studio sulla valutazione del rischio fiscale

Riassunto: Il *data mining* e l'intelligenza artificiale sono sempre più utilizzati nell'analisi dei dati. L'ideale sarebbe ottenere un'automazione completa, ma in molte applicazioni ciò comporta rischi significativi. In questi casi è necessario il coinvolgimento diretto di analisti umani per raffinare l'analisi o per prendere le decisioni finali. Un problema rilevante è quindi come garantire un processo decisionale efficiente e affidabile nel quale gli esseri umani sono parte integrante del processo di analisi. Proponiamo una metodologia *human-in-the-loop* che sfrutta il *data mining*, il *machine learning*, e la visualizzazione per migliorare il processo di analisi. Un elemento chiave è l'uso di una *dashboard* visuale intuitiva, di supporto all'individuazione di relazioni e pattern di dati nascosti. Come caso di studio, descriviamo un'applicazione di questa metodologia per l'analisi del rischio fiscale nell'ambito delle attività dell'Agenzia delle Entrate.

Keywords: *Human-in-the-loop* – *Data mining* – Analisi visuale – Visualizzazione di reti – Valutazione del rischio fiscale

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0089
Articolo sottoposto a peer review

Legalità, algoritmi e corruzione: le tecniche di intelligenza artificiale potrebbero essere utilizzate *nel* e *per* il sistema di prevenzione della corruzione?

Francesco Merenda

L'articolo vuole ragionare su quali potrebbero essere i vantaggi e i rischi legati all'impiego delle tecniche di intelligenza artificiale (IA) nel sistema italiano della prevenzione della corruzione. In particolare, ci si sofferma sul processo di gestione del rischio, quale momento cruciale per l'adozione delle misure amministrative di prevenzione della corruzione. L'utilizzo di tecniche IA potrebbe, infatti, perfezionare queste fasi, velocizzare la procedura e garantire maggiore imparzialità nella scelta delle misure. Al contempo però l'adozione di tecniche IA, parziali o totali, porterebbe con sé sia alcuni aspetti problematici sia un significativo ridimensionamento del sistema vigente. Una seconda riflessione è dedicata a quei settori o strumenti che, sebbene non siano da reputare strettamente interni al sistema della prevenzione, potrebbero contribuire alla causa preventiva stessa. Nella parte finale si ragiona sulle conseguenze più difficili che l'applicazione dell'intelligenza artificiale nel campo della prevenzione potrebbe comportare in termini di partecipazione e legalità.

Intelligenza artificiale – Prevenzione della corruzione – Legalità – Partecipazione

Sommario: *Premessa – 1. I motivi che legittimano il ricorso all'IA nel sistema dell'anticorruzione italiano – 2. Campi e strumenti che potrebbero avvalersi dell'IA* per *il sistema di prevenzione – 2.1. Le procedure di reclutamento del personale della PA – 2.2. Perfezionamento degli indici* red flags *– 2.3. Investimento nel cd.* e-procurement *per prevenire ed individuare la corruzione negli appalti pubblici – 2.4. Utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di* whistleblowing *– 3. Alcune esperienze concrete di applicazione IA* nel *campo anticorruzione a livello globale – 4. Quali sfide e rischi ne derivano in termini di legalità e partecipazione? – 4.1. Segue. Prevenzione della corruzione e partecipazione – 5. Riflessioni conclusive*

Premessa

È ormai appurato che la pubblica amministrazione si doterà sempre di più di tecniche e strumenti basati sugli algoritmi e, di conseguenza, ci si interroga, in particolare, se l'intelligenza artificiale verrà ampiamente sfruttata anche nel campo della prevenzione della corruzione.

Questo scenario è stato ipotizzato da alcuni studiosi[1] in quanto, attraverso la sostituzione della decisione umana con quella della macchina, si potrebbe garantire un maggior rispetto del principio d'imparzialità e della legalità stessa. Anche gli organismi internazionali, negli ultimissimi anni, hanno raccomandato sempre di più l'utilizzo di nuovi approcci basati sui dati per migliorare la valutazione del rischio di corruzione[2] nel settore pubblico.

Partendo da una definizione standard di intelligenza artificiale come quell'insieme di tecnologie in

F. Merenda è dottorando di ricerca in "Legalità, Culture politiche e Democrazia" presso il Dipartimento di Scienze politiche dell'Università degli studi di Perugia. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

cui le macchine imitano l'intelligenza umana per risolvere problemi complessi, sorgono spontanee alcune domande: i problemi legati alla scarsa effettività delle misure anticorruzione sono da reputare complessi? E ancora, l'impiego esteso delle tecniche IA nella definizione delle misure dei Piano triennale di prevenzione della corruzione e della trasparenza (di seguito Ptpct) e di altre azioni preventive potrebbe diventare una componente stabile di quella che sarà la cd. "amministrazione intelligente"[3]?

1. I motivi che legittimano il ricorso all'IA nel sistema dell'anticorruzione italiano

Occorre, in via preliminare, affermare che la risposta alla domanda che funge da titolo del presente lavoro è affermativa, in quanto questa frontiera è già stata sperimentata in alcuni ordinamenti giuridici. È alquanto interessante invece capire in che modo ciò si potrebbe applicare e se ci saranno concreti progressi per il sistema preventivo della corruzione italiano. Appare dunque ragionevole chiedersi, soprattutto attraverso una prospettiva giuridica, quali sarebbero gli eventuali benefici e problemi derivanti dall'utilizzo di queste tecnologie.

Sono essenzialmente tre le principali cause che giustificano l'impiego delle tecniche di intelligenza artificiale in questo campo: a) l'insufficienza e i limiti dell'attuale sistema dell'anticorruzione italiano; b) i miglioramenti in termini di imparzialità; c) l'efficientamento e la semplificazione delle procedure di approvazione dei Ptpct.

Il sistema di prevenzione amministrativa della corruzione[4] pone una riflessione sull'effettività delle misure adottate per questa politica, anche alla luce dell'imminente ricorrenza del primo decennio dall'entrata in vigore della legge anticorruzione n. 190/2012. È dunque, oggi, possibile trarre un bilancio dell'impatto prodotto da questa policy, mettendo in rilievo luci e ombre derivanti dalla prassi applicativa delle pubbliche amministrazioni.

Il framework dell'anticorruzione è basato su un impianto "centro-periferico", dove gli indirizzi vengono emanati dall'autorità nazionale anticorruzione e l'attuazione è affidata alle singole amministrazioni, secondo una logica *bottom-up*; l'implementazione del sistema invece poggia su due principali pilastri, che sono i Ptpct e i doveri di comportamento: i primi consistono in una serie di misure *ad hoc* adottate dalle pubbliche amministrazioni dopo un processo preliminare di analisi del rischio e in base al piano nazionale anticorruzione (Pna); le regole di condotta, invece, sono sancite nei codici di comportamento dei dipendenti pubblici, oltre a quelle previste da alcune leggi.

Sin dalla prima esperienza applicativa sono emerse alcune criticità di quest'impianto relativamente ad alcuni fattori: le misure dei Ptpct spesso vengono adottate con approccio "adempimentale" quindi non risultano in linea con l'obiettivo di analisi e gestione del rischio; le regole sancite nei codici di comportamento, che dovrebbero introdurre doveri integrativi e coerenti con il tipo di amministrazione, sono il risultato di un puro esercizio esteriore; la formazione, che è un fattore centrale[5], sollecitato a livello internazionale, ha assunto la forma e la sostanza di meri momenti ritualistici e dunque improduttivi nella prospettiva di creazione e diffusione di una cultura dell'integrità e dell'anticorruzione; ultimo ma non meno importante, il nostro sistema anticorruzione continua a mostrarsi non del tutto in linea con il concetto di integrità pubblica raccomandato dall'Ocse[6], il quale si basa su un approccio che vede nelle politiche anticorruzione una componente centrale, ma che va necessariamente coadiuvata con altre politiche nel settore pubblico: la promozione dell'efficienza amministrativa e il raggiungimento dei risultati; la diffusione di un settore pubblico professionale e fondato sul merito; incoraggiare una cultura organizzativa aperta; investire in una leadership etica e diffondere una cultura dell'integrità.

Quale IA[7] per l'ambito di prevenzione? L'intelligenza artificiale si distingue in due macro-tipologie: l'*artificial general intelligence* (AGI) e l'*artificial narrow intelligence* (ANI). La prima è stata definita come «una macchina e o un sistema che può eseguire solo un compito strettamente definito o un piccolo insieme di compiti correlati»[8]; la seconda invece come «una macchina in grado di comprendere il mondo come qualsiasi essere umano e con la stessa capacità di imparare a svolgere un'enorme gamma di compiti»[9].

Nel caso in questione, ma ad oggi in generale nella maggioranza dei campi, quando si parla di utilizzare queste tecniche ci si riferisce principalmente all'AGI, la quale a sua volta è composta da due categorie principali di programmazione: *rule-based programming* e il *machine learning*[10]. La prima forma di programmazione si basa su un processo secondo il quale i programmatori umani scrivono un codice che stabilisce le regole che definiscono tutti gli aspetti di una determinata attività (per es. se succede il fenomeno β, allora ne consegue una specifica risposta δ, se si verifica una situazione diversa da β, allora ne consegue γ). La seconda forma è costituita da macchine che non dipendono dai dati, bensì imparano dai dati e dall'esperienza, un sottocampo di questa forma di programmazione è il cd. *deep learning* formato da modelli di apprendimento automatico detti reti neurali[11].

In merito alla seconda tipologia di programmazione si nutrono maggiori perplessità e osservazioni critiche: sebbene siano più veloci ed accurate, l'opacità interna al funzionamento di questi dispositivi non permetterebbe di rendere trasparenti e spiegabili i passaggi che partono dalle premesse e arrivano ai risultati[12].

Le prime esperienze di applicazione dell'IA quindi si inseriscono nel campo dell'*artificial general intelligence*, sebbene vi siano casi[13] in cui si utilizzano sia la programmazione *rule-based programming* che quella *machine learning*.

La *conditio sine qua non* perché si possa arrivare a buone decisioni automatizzate nel campo della prevenzione della corruzione è ovviamente legato all'uso dei big data[14], consistente in un numero infinito di informazioni e dati. Si può dire infatti che gli algoritmi senza dati sono vuoti e i dati senza algoritmi sono ciechi[15]. L'utilizzo dei big data servirebbe quindi per fare scelte più efficienti e intelligenti nel rispetto del principio di legalità[16]. Ciò però dovrebbe essere sviluppato in concomitanza con una pubblica amministrazione che sia sempre più digitale e, quindi, soltanto dopo aver superato l'attuale *digital gap*[17]. Tale divario è amplificato dalle poche risorse impiegate finora per studiare in modo approfondito l'IA, soprattutto in termini di ricerca e sviluppo[18]. Il raggiungimento di questi obiettivi, pertanto, è imprescindibile affinché si possano adoperare strumenti e modelli IA.

Il binomio intelligenza artificiale-big data potrebbe rappresentare il miglior utilizzo delle ICT nel campo dell'anticorruzione: con l'ausilio del *machine learning* e del *deep learning* si potranno fare analisi di dati molto precise fino a permettere l'individuazione di correlazioni e anomalie all'interno di vasti *dataset*.

Prima di ipotizzare quali potrebbero essere gli ambiti ad avvantaggiarsi dell'IA è bene ragionare anzitutto sui potenziali effetti positivi in termini di imparzialità ed efficienza della pubblica amministrazione (di seguito anche PA).

L'impiego di algoritmi predittivi potrebbe favorire il modello di legalità efficiente della PA all'interno del processo di adozione dei Ptpct?

Per quanto concerne il principio di imparzialità, *prima facie*, la risposta immediata non potrebbe che essere positiva. La cd. "decisione robotica" garantirebbe maggiore imparzialità nella scelta rispetto a quella umana che peraltro per sua natura potrebbe essere influenzata[19] e che spesso non tiene in considerazione che la scelta è una responsabilità[20]. L'automatizzazione e la spersonalizzazione delle scelte eliminano i rischi umani e i cattivi comportamenti dei funzionari e ciò rappresenterebbe una valida garanzia per la prevenzione della corruzione.

Nel processo di definizione delle misure e nella fase preliminare di analisi del rischio dei Ptpct l'IA potrebbe facilitare l'individuazione delle misure che l'amministrazione adotterà al fine di incentivare le buone condotte del personale, assicurando di conseguenza una maggiore imparzialità nelle scelte fatte.

Il Codice dell'amministrazione digitale italiano (d.lgs. 7 marzo 2005, n. 82), precisamente al comma 1 dell'art. 12, afferma che le pubbliche amministrazioni utilizzano le ICT per la realizzazione degli obiettivi di imparzialità, ma anche quelli di efficienza, efficacia, economicità, trasparenza, semplificazione e partecipazione[21].

Si deve però precisare che l'imparzialità di cui si parla è da circoscrivere alla sola fase di predisposizione delle misure organizzative dei piani di prevenzione. Garantito ciò, però, l'imparzialità soggettiva dei funzionari, quale pietra angolare del sistema di prevenzione italiano, continuerebbe a dipendere dalle condotte di chi lavora alle dipendenze della PA. Tale precisazione è necessaria per sottolineare che, anche se le ipotesi in discussione si dovessero concretizzare, la responsabilità del rispetto delle misure e dei doveri, ma anche di efficacia del sistema complessivo, rimane affidata al personale dell'amministrazione.

Oltre all'imparzialità, potrebbero trarre beneficio dall'applicazione di tecniche di IA anche l'attuazione del principio di buon andamento e i suoi corollari.

Già il Consiglio di Stato nel 2019[22] ha affermato che l'utilizzo di siffatte tecniche è conforme con i canoni di efficienza ed economicità dell'azione amministrativa, in particolare grazie: «alla 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».

2. Campi e strumenti che potrebbero avvalersi dell'IA *per* il sistema di prevenzione

Osservando l'iter delle varie fasi dell'adozione dei Ptpct ci si rende facilmente conto che le risorse impiegate sono tante e il personale coinvolto detiene diversi compiti e responsabilità. Ogni attore coinvolto, inoltre, dispone di dati utili e rilevanti che debbono essere forniti con tempestività al Responsabile della prevenzione (Rpct). Già in questa fase, quindi, le risorse di vario tipo potrebbero essere risparmiate, le tempistiche drasticamente ridotte e la gestione dei dati migliorata attraverso l'utilizzo delle tecniche *blockchain*[23].

Si tratta di registri distribuiti che permettono di gestire e aggiornare un registro di dati e informazioni in modalità aperta, condivisa e distribuita senza un controllo centrale e di verifica. In questo modo, oltre ai vantaggi appena detti, si garantirebbe di conseguenza una più rapida e proficua analisi del contesto interno ed esterno. I registri distribuiti permetterebbero quindi una migliore gestione delle fonti dei dati per l'analisi di contesto[24], incidendo in positivo sia sull'individuazione e la mappatura dei processi che sull'identificazione di quei dati che potrebbero contenere le caratteristiche organizzative capaci di avere influenza sul profilo di rischio dell'amministrazione.

Un altro significativo apporto dell'IA potrebbe consistere nella possibilità di perfezionare e rendere più attendibili gli indicatori di monitoraggio e anche i cd. *key risk indicators*, utili a fornire indicazioni sul livello di esposizione al rischio del processo o delle sue attività componenti. La definizione di questi indicatori è preliminare al processo vero e proprio: grazie ai dati raccolti in precedenza, l'IA e il *machine learning* riuscirebbero ad elaborare più rapidamente gli indicatori, che sarebbero più precisi ed efficaci.

Inoltre, l'IA potrebbe essere assunta come nuova tecnica per l'individuazione degli eventi corruttivi che si basano su analisi di documenti e banche dati. Ciò consentirebbe una più rapida ed attendibile identificazione e formalizzazione dei rischi, utili per la creazione del "registro degli eventi rischiosi" nel quale per ogni processo si deve individuare almeno un rischio. Le tecniche algoritmiche potrebbero garantire maggiore analiticità e far corrispondere meglio i rischi alle varie fasi del processo. Tuttavia, bisogna considerare che, se da un lato le procedure automatizzate garantirebbero maggiore rapidità e analiticità, dall'altro non sarebbero però capaci di descrivere gli eventi rischiosi che, ad oggi, è un tratto peculiare del processo di costruzione del registro stesso.

Un ultimo contributo, ma forse il più determinante, potrebbe essere quello nella fase di scelta dell'approccio valutativo (qualitativo, quantitativo o misto). Ad oggi, l'ANAC consiglia[25] la scelta di un metodo qualitativo, dato che quello quantitativo è basato su analisi statistiche o matematiche e sebbene abbia il pregio di quantificare il rischio attraverso i numeri al contempo le amministrazioni non hanno né personale capace di fare ciò né serie storiche adeguate. Lo sviluppo futuro di *machine learning* e di reti neurali potrebbe rivelarsi utile anche a questo fine, consentendo quindi di propendere per la scelta di questo metodo valutativo.

Un discorso a parte, invece, riguarda la fase di valutazione del rischio in senso stretto, laddove si identificano i comportamenti che potrebbero essere fonte di fatti corruttivi. Infatti, se da un lato l'ausilio dell'algoritmo potrebbe essere utile per affinare la valutazione di esposizione al rischio attraverso gli indicatori di rischio stessi, da un altro lato, però, il contributo degli attori umani rimane determinante nelle restanti fasi del processo. L'ipotesi fino ad ora presa in considerazione concerne le prime due macrofasi del processo di gestione del rischio ("Analisi del contesto" e "Valutazione del rischio"), dove l'utilizzo delle tecniche di IA è considerato possibile e perfino vantaggioso. Nella terza macro-fase ("Trattamento del rischio"), invece, l'impiego dell'IA non è ritenuto necessario, poiché la funzione svolta nella procedura dagli attori coinvolti risulta essere imprescindibile.

Ad ogni modo, da quanto detto conseguirebbe un cambiamento netto del processo: l'algoritmo sostituirebbe la scelta di molte determinazioni degli interventi organizzativi da adottare nel campo della prevenzione della corruzione.

Sulla base di queste osservazioni si possono brevemente immaginare due possibili scenari: il primo basato su un utilizzo ponderato dell'intelligenza artificiale, ovvero limitatamente ad alcuni campi; l'altro, invece, dove tutte le determinazioni vengono decise dalle procedure automatizzate.

Nel primo caso si tratterebbe quindi di utilizzare il modello di programmazione algoritmica nel seguente modo: di fronte ai rischi x si individuano le misure y, le quali vengono individuate in un'amministrazione attraverso una sequenza logica predeterminata e condizionata dal programmatore.

Quindi, come si può notare, questo tipo di intervento non è definibile come una tecnica di IA pura, in quanto l'elemento umano sarebbe presente e determinante nella fase di programmazione. Questo tipo di utilizzo potrebbe apportare maggiore oggettività e imparzialità della scelta delle misure da adottare, senza eliminare del tutto il contributo dei funzionari.

L'elemento umano continuerebbe a svolgere un ruolo significativo nello sviluppo delle varie fasi della policy anticorruzione. Si verrebbe dunque a prospettare un rapporto tra PA e IA conforme ai principi di sviluppo etico dell'IA[26] e coerenti con la logica *govern IA and govern with IA*[27]. Tale approccio sarebbe d'altronde in linea con quanti nella dottrina italiana, in merito a siffatte questioni, sostengono l'indispensabilità del funzionario umano[28].

Diversamente dal primo scenario, qualora si riuscissero ad applicare diffusamente le tecniche di intelligenza artificiale si avrebbero significativi cambiamenti sul vigente processo di gestione del rischio: alcune fasi sarebbero fortemente condizionate dal ricorso alle tecniche IA, alcune verrebbero semplificate e altre eliminate del tutto; il ruolo di alcuni attori verrebbe vanificato dal contributo dell'IA; infine anche la scelta

delle misure concrete da adottare per la prevenzione dei rischi subirebbe una significativa variazione, dato che questa parte della procedura è influenzata dall'analisi svolta in precedenza.

Rimanendo all'ipotesi sopra esposta, infatti, la scelta delle misure dev'essere descritta con accuratezza per porre in rilievo sia l'obiettivo che si intende raggiungere che le modalità adoperate. Stessa cosa è valida per il conseguente processo di programmazione delle misure. Tutto ciò, stando a questa seconda ipotesi, non potrebbe essere garantito e ciò desta non poche perplessità. Questa considerazione, tuttavia, non riguarda solo l'ambito dell'anticorruzione, bensì la possibile applicazione estesa dell'IA, e nello specifico del *machine learning*, nel contesto dell'attività della pubblica amministrazione. In particolare, tali dubbi riguardano le questioni relative sia alla motivazione[29] di come si giunge ad un data soluzione sia in merito all'esplicitazione dei fattori che determinato la scelta[30] e se si tratta di un sistema basato sull'apprendimento occorre specificare il metodo di addestramento dell'algoritmo utilizzato.

Detto ciò, comunque, non si può escludere che in futuro alcune tecniche IA di questo tipo possano essere adoperate come misure di prevenzione della corruzione. Infatti, le ipotesi sopra avanzate si riferiscono esclusivamente al sistema di definizione dei Ptpct. Meritano invece un discorso a parte quelle misure che grazie all'IA potrebbero, e in alcuni Stati già lo fanno, rappresentare un valido contributo alla causa preventiva della corruzione in senso più ampio.

Oltre alle misure che vengono adottate *nel* sistema di prevenzione (Ptpct) vero e proprio, vi sono inoltre settori in cui l'applicazione di queste tecnologie potrebbe parimenti influire sul sistema di prevenzione. Si tratta di strumenti e settori che, nonostante non siano interni all'impianto preventivo, costituiscono un valido e necessario apporto alla causa dell'integrità della pubblica amministrazione.

I principali ambiti potrebbero essere i seguenti: le procedure di reclutamento del personale della PA; il perfezionamento degli indici *red flags*; l'investimento nel cd. *e-procurement* per prevenire ed individuare la corruzione negli appalti pubblici; l'uso della *blockchain* come strumento per maggiore trasparenza, efficienza e garanzia per l'amministrazione digitale; utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di *whistleblowing*.

2.1. Le procedure di reclutamento del personale della PA

Il reclutamento del personale è considerato dall'ANAC come una delle principali aree di rischio[31] e dunque oggetto di particolare attenzione nell'ottica della prevenzione della corruzione. Infatti, trasparenza e imparzialità sono i requisiti centrali in materia di assunzione del personale all'interno della legge anticorruzione del 2012[32].

È da ormai un anno che si stanno sperimentando nuovi meccanismi per la selezione dei candidati nei concorsi pubblici. Tale aspetto si pone in conformità con l'art. 35 del d.lgs. 30 marzo 2001, n. 165, che nel regolare il reclutamento del personale, al comma 3 prevede che la PA può ricorrere: «all'ausilio di sistemi automatizzati, diretti anche a realizzare forme di preselezione».

L'art. 10 del d.lgs. 28 maggio 2021, n. 76[33] ha aperto alle tecniche di IA nell'ambito delle procedure concorsuali per garantire maggiore velocità, efficienza e soprattutto maggior aderenza ai princìpi costituzionali che regolano l'accesso ai pubblici uffici[34].

Le riflessioni debbono essere fatte in termini di costi/benefici: da un lato, la velocizzazione della tempistica di selezione, della correzione delle prove e la possibilità immediata per il candidato di verificare i risultati; dall'altro, emergono alcuni rischi legati al rispetto di una serie di princìpi delicati.

Le maggiori ricadute positive riguardano sia la procedura che la stessa scelta dei candidati. Lo svolgimento delle prove beneficerebbe di una significativa semplificazione, ma anche una più rapida attribuzione dei risultati ai candidati e quindi si giungerebbe più rapidamente alla formazione delle graduatorie. Da questo punto di vista, dunque, si otterrebbero effetti positivi relativamente sia al buon andamento che all'imparzialità. In quanto, quest'ultimo principio sarebbe garantito dal fatto che nel momento di correzione delle prove verrebbero eliminati sia gli eventuali errori che l'indebita interferenza umana. Si potrebbe dunque ottenere maggiore imparzialità nella scelta dei candidati, per questo motivo ciò potrebbe rappresentare il maggiore vantaggio per la procedura di selezione nella prospettiva della prevenzione dei fatti corruttivi.

La giurisprudenza costituzionale ha designato un vero e proprio rapporto strumentale tra la regola del concorso pubblico e il principio di buon andamento[35], ciò si traduce nell'esigenza che le amministrazioni possano dotarsi di personale idoneo per svolgere le funzioni ad essi affidate. L'automatizzazione delle varie fasi concorsuali, attraverso per esempio l'utilizzo di software a lettura ottica OCR consistenti in riconoscimento ottico dei caratteri, comporta un risparmio di tempo, di impiego di risorse di vario tipo e quindi renderebbe l'iter più efficiente ed efficace per quanto riguarda la formazione delle graduatorie nel più breve tempo possibile.

Un altro aspetto positivo è quello che ogni candidato e candidata potrebbero tempestivamente verificare il proprio punteggio e le risposte non corrette, così da poter accedere agli atti (l. 7 agosto 1990, n. 241) senza l'intervento della PA.

I rischi invece sono legati al rispetto di princìpi molto importanti: alcuni di essi sono interni al già citato comma 3 dell'art. 35 del d.lgs. 165/2001 e altri contenuti nel GDPR[36]. Nel primo caso, le maggiori preoccupazioni riguardano il principio di pari opportunità tra lavoratrici e lavoratori sancito alla lettera c) del comma 3 dell'art. 35 del d.lgs. 165/2001. Infatti, in tal senso si sono verificati problemi simili nell'esperienza statunitense[37]: gli algoritmi non avrebbero considerato la parità di genere nel processo di elaborazione degli output. Anche se le discriminazioni potrebbero essere anche di altri tipi[38]. I problemi legati al GDPR sono rappresentati innanzitutto dall'art. 22 (*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*)[39], dal quale deriva che nei concorsi pubblici bisognerebbe garantire ai candidati una valutazione che non sia totalmente effettuata dai meccanismi automatizzati. Ulteriori preoccupazioni sono dovute alla poca trasparenza del processo di elaborazione del risultato, al trattamento dei dati personali[40] ed al principio di controllo atto a garantire che gli individui siano attori informati e in controllo delle loro scelte[41].

La recente esperienza applicativa dell'IA ai concorsi pubblici evidenza vantaggi e pericoli, che potrebbero essere però superati attraverso l'utilizzo di metodi che proteggano i dati e i princìpi succitati, soprattutto attraverso una chiara regolamentazione.

2.2. Perfezionamento degli indici *red flags*

Sempre nell'ottica di miglioramento dell'analisi del rischio corruttivo, l'ANAC ha promosso, anche attraverso le tecniche IA, alcune ricerche ed iniziative mirate a sviluppare indicatori di rischio più efficaci e distinti per settori e tipologie di amministrazioni[42]. Gli indici *red flags* o indicatori di rischio sono misure sintetiche composte da una o più variabili, che identificano l'esistenza del rischio di corruzione all'interno di specifici processi decisionali[43].

Ad oggi, alcuni studi[44] hanno ipotizzato l'utilizzo di *machine learning* per lo sviluppo di indici capaci di prevedere la corruzione, in particolare nel settore degli appalti pubblici. Sostanzialmente ci si basa su enormi banche dati che raccolgono i vari dati (per es. gli acquisti pubblici) e poi attraverso le tecniche di intelligenza artificiale producono gli indici di rischio. Gli algoritmi identificano e segnalano in modo indipendente quei modelli sospetti che emergono dai dati e li segnalano a coloro che si occupano dei controlli interni ed esterni all'amministrazione Il problema derivante da ciò, come in tutti gli altri casi in cui si utilizzano grandi banche dati[45], è quello della tutelabilità e titolarità del bene posto dalla natura immateriale delle banche dati. Più in generale, verrebbero a configurarsi quegli aspetti problematici legati alla finalità del trattamento dei dati[46], la lesione del diritto all'autodeterminazione informativa e quindi il rispetto delle disposizioni della normativa privacy sancita dal Regolamento UE n. 2016/679 (GDPR)[47].

Gli scenari, anche in questo caso, sono diversi in virtù del rapporto tra le tecniche IA e gli attori umani[48]: in un primo scenario, le tecnologie adoperate raccolgono le informazioni, che necessitano della presenza degli analisti umani per rilevare le pratiche corrotte evincibili dai dati; un secondo scenario è quello che consente agli algoritmi di identificare in modo indipendente i modelli sospetti nei dati e segnalarli successivamente agli attori imputati al controllo. Un terzo e per ora più remoto scenario è quello che attribuisce maggiore autonomia agli algoritmi, i quali non solo potrebbero effettuare il processo di rilevazione in modo indipendente, ma anche pubblicare automaticamente i casi sospetti. Senza la presenza degli attori di controllo, tuttavia, le informazioni raccolte dalle tecniche IA potrebbero non tenere conto del fatto che alcune di esse riguardino dati personali che si riferiscono a una persona identificata o identificabile[49]. Un tale scenario si pone inoltre in contrasto con l'art. 22 del GDPR che vieta, come detto, la possibilità che la decisione venga unicamente assunta dai sistemi automatizzati.

In questa ipotesi, pertanto, potrebbero configurarsi rischi concreti per la privacy a causa dell'applicazione totale dell'IA, dove gli attori umani avrebbero unicamente un ruolo marginale, ovvero successivo al processo di rilevazione.

Gli indici *red flags*, quindi, potrebbero essere perfezionati attraverso set di dati, elaborati dagli strumenti IA, utili alla individuazione dei problemi[50]. Il potenziamento di questi indici potrebbe non solo costituire un valido e robusto ausilio alle amministrazioni nel loro processo di monitoraggio e prevenzione del rischio, ma potrebbe anche sviluppare un sistema che sia maggiormente in raccordo con il processo di misurazione e valutazione della performance[51].

2.3. Investimento nel cd. *e-procurement* per prevenire ed individuare la corruzione negli appalti pubblici

I recenti scandali legati agli appalti nel periodo della pandemia hanno riacceso l'attenzione sulla necessità

di potenziamento del sistema di regolamentazione e controllo di questo settore.

Il Pnrr ha incluso tra i principali obiettivi quello di far evolvere il sistema di *e-procurement* attraverso la digitalizzazione *end-to-end* dei processi di approvvigionamento pubblico[52] ed in particolare di utilizzare: «intelligenza artificiale/machine learning per l'osservazione e l'analisi delle tendenze nell'uso degli strumenti di acquisto, delle dinamiche di mercato e di spesa e dei comportamenti di pubblica amministrazione e operatori economici[53]».

Esistono già studi e primi approcci[54] (su uno di essi si dirà meglio nel paragrafo successivo) circa il possibile contributo che le tecniche IA potrebbero dare alla causa dell'anticorruzione nella sfera degli appalti pubblici. L'affinamento degli indici *red flags*[55] è in realtà solo una delle componenti che potrebbe costituire un vero e proprio irrobustimento del, già esistente, sistema di *e-procurement*.

Nella prospettiva anticorruzione, l'ausilio di meccanismi IA potrebbe comportare vantaggi di tipo incrementale, senza però alterare in modo significativo (o sostituire) le architetture di supervisione e applicazione esistenti[56]. L'IA insomma potrebbe aiutare in termini di controllo e di individuazione della potenziale corruzione ed esonerare gli attori umani da tale compito.

Anche nel settore del *public procurement*, quindi, l'IA non apporterebbe modifiche rivoluzionarie rispetto alle attuali modalità di prevenzione e controllo previste dalla disciplina italiana. Il maggiore vantaggio consisterebbe nell'offrire un notevole incremento e accelerazione dei controlli anticorruzione, con il beneficio di poter effettuare in anticipo i relativi interventi.

L'utilizzo del *machine learning* e le tecniche di *text-mining*[57] si basano su cospicue fonti di dati, tipo quelli contenuti nelle documentazioni di gara, per poter individuare segnali di corruzione nel processo degli appalti[58].

La tecnologica *blockchain* potrebbe essere un ulteriore valore aggiunto per il rafforzamento dell'*e-procurement*, soprattutto in merito ad un potenziamento della digitalizzazione delle procedure di affidamento degli appalti già in vigore e degli acquisti. In tal modo, si avrebbe senz'altro un miglioramento dei princìpi di imparzialità e buon andamento, ma consentirebbe anche di far sì che questi metodi siano quelli prevalenti nell'attività delle stazioni appaltanti. Per giunta, i registri distribuiti potrebbero risultare utili per la gestione dei dati degli operatori economici e per accelerare l'attività istruttoria della stazione appaltante. La finalità di questo tipo di intervento è quello di scongiurare la presenza di false dichiarazioni all'interno dei documenti di gara e inoltre per limitare la relativa valutazione discrezionale da parte della stazione appaltante.

2.3.1. L'uso della blockchain *come strumento per maggiore trasparenza, efficienza e garanzia per l'amministrazione digitale*

Rispetto ai registri *blockchain*, si è già detto che potrebbero fungere da maggiore promessa di trasparenza generale per la PA, ma si riportano tuttavia i benefici specifici derivanti da essi: tracciamento sicuro e trasparente delle informazioni e dei dati; immodificabilità e tracciabilità nella gestione dei dati; utilizzabilità e validità in diversi ambiti; maggiore automatizzazione dei processi; rafforzamento della fiducia tra cittadini e le pubbliche amministrazioni; migliore e più efficiente gestione documentale; maggiore interoperabilità tra le varie PA; maggiore trasparenza dei processi interni.

Da queste conseguenze positive ne deriva che il sistema di prevenzione della corruzione potrebbe essere uno dei settori più idonei a sfruttare le potenzialità messe a disposizione da questi registri. Le tecnologie *blockchain* stanno attirando le comunità anticorruzione per il loro potenziale di prevenzione della corruzione e per la garanzia di protezione dei registri pubblici da frodi e manomissioni[59]. La *blockchain* scongiura la probabile manomissione dei registri, in quanto non consentirebbe ai dipendenti di apportare modifiche e falsificare le voci interne ad essi.

È dunque auspicabile che la pubblica amministrazione italiana e l'ambito di prevenzione possano usufruire diffusamente di questo sistema, soprattutto nella prospettiva dell'auspicata trasparenza algoritmica[60].

2.4. Utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di *whistleblowing*

In tema di segnalazioni anonime di illeciti, l'ordinamento italiano è tuttora in corso di adeguamento alla direttiva (UE) 2019/1937 in materia di *whistelblowing*. A parte ciò, è auspicabile anche in questo campo l'adozione dell'IA per le procedure di acquisizione e gestione delle segnalazioni anonime.

L'attuale disciplina italiana si sviluppa in concreto con la presentazione delle segnalazioni mediante diversi canali, anche se l'utilizzo della piattaforma è ritenuto prioritario.

La procedura si basa su un protocollo di crittografia, che è un sistema basato sull'uso di un algoritmo matematico che agisce su una serie di caratteri. Tale sistema garantisce il trasferimento di dati riservati e, in seguito alla segnalazione, genera un codice identificativo univoco registrato sul portale ANAC, che permette

al *whistelblower* di comunicare in modo anonimo con l'autorità. I dati che vengono comunicati sono poi segregati all'interno di un'apposita sezione della piattaforma, la quale è inaccessibile anche all'ufficio per la vigilanza sulle segnalazioni dei *whistleblowers* (UWHIB). Questa procedura assicura maggiore riservatezza e celerità delle procedure, anche se ad oggi, nonostante questa tipologia sia quella raccomandata dall'ANAC, non è imposta nell'attuale l. 30 novembre 2017, n. 179[61]. Anche nelle linee guida ANAC del 2021, quando si parla di modalità di gestione delle segnalazioni, si afferma che: «le Amministrazioni sono, quindi, tenute a disciplinare, in conformità alle presenti Linee guida, le procedure, preferibilmente informatizzate, per la ricezione e gestione delle segnalazioni».

Appare essenziale investire solo su questo tipo di tecnologie ai fini di una maggiore conformazione ai princìpi sanciti all'art. 9 della direttiva del 2019 e per superare alcuni problemi recentemente sollevati dal Garante della privacy[62].

Le tecniche IA potrebbero servire per perfezionare l'operazione di crittografia attualmente adoperata. Per esempio, ci sono modelli proposti che basano le procedure di segnalazione sul sistema *blockchain*, che si avvale di una crittografia asimmetrica. In particolare, le proprietà dei registri distribuiti e l'affidabilità delle cd. *ring signatures* creerebbero maggiori condizioni favorevoli non solo per la procedura stessa, ma potrebbero infondere maggiore fiducia e incentivi al *whistleblower*[63] nell'effettuare la segnalazione.

3. Alcune esperienze concrete di applicazione IA *nel* campo anticorruzione a livello globale

Il recente sviluppo di iniziative basate su strumenti IA, finalizzate a perfezionare le strategie anticorruzione, ha creato un alto livello di aspettative[64], ma ha consentito inoltre una prima comprensione su vantaggi e difficoltà derivanti da queste nuove pratiche[65].

Si descrivono sinteticamente le seguenti esperienze: il sistema di allerta precoce dei ricercatori dell'Università di Valladolid; l'operazione *Serenada de amor* in Brasile; *ProZorro* in Ucraina nel campo dell'*e-procurement*.

Il sistema di allerta precoce dei ricercatori dell'Università di Valladolid

Due ricercatori dell'Università di Valladolid hanno sviluppato un modello basato su reti neurali, attraverso mappe auto-organizzate, per prevedere in quali province spagnole[66] potrebbero verificarsi casi di corruzione[67], sulla base di vicende che sono state affrontate dai media o che sono già andate a processo.

Il sistema fornisce alcuni dati che indicano un'alta probabilità di corruzione, anche se gli stessi autori tengono a sottolineare che ciò non significa che la corruzione accada effettivamente. Dallo studio emerge che ci sono una serie di fattori economici e politici che consentono di creare un attendibile sistema di allerta precoce. I principali fattori che favorirebbero la corruzione sono: la tassazione e l'aumento dei prezzi degli immobili, la crescita economica, il numero crescente di istituti di deposito e società non finanziarie; la presenza di uno stesso partito politico al potere per lunghi periodi. Occorre però riportare alcune precisazioni sui fattori appena indicati. La crescita economica o il fatto che un determinato partito rimane al potere a lungo non sono direttamente cause di corruzione pubblica. La ricerca considera invece che le zone a più rapida crescita o quelle governate dallo stesso partito per lungo tempo potrebbero essere più soggette a casi di corruzione. La crescita economica, quindi, non è un pericolo o un fattore corruttivo di per sé, ma laddove si verifica aumentano le interazioni tra gli agenti economici e i funzionari pubblici e questo potrebbe determinare anche l'insorgere di alcune relazioni opache. Stessa cosa è valida per i partiti che rimangono a lungo tempo al potere: tale situazione potrebbe favorire la presenza di rapporti clientelari e sleali tra i politici e gli operatori economici. Mentre la presenza di mercati più competitivi può comportare la diffusione di influenze di agenti che vogliono ottenere a tutti i costi, ad esempio attraverso tangenti o la promessa di compensi di ogni tipo, concessioni o affidamenti di varia natura.

Tale sistema fornisce diversi profili di rischio di corruzione a seconda delle condizioni economiche di una regione e della tempistica della previsione: consente infatti di prevedere la corruzione fino a tre anni prima che i casi vengano rilevati, in altri casi fornisce previsioni più nel breve termine e in questi casi gli studiosi suggeriscono l'adozione di misure preventive più urgenti.

Lo studio si è basato su tutti i casi di corruzione comparsi in Spagna tra il 2000 e il 2012, tra cui casi celebri come il caso Mercasevilla e il caso Baltar. Il metodo di raccolta e di analisi delle informazioni è stato eseguito con le reti neurali, che hanno consentito di rilevare i fattori più predittivi di corruzione.

Il principale punto di forza e di innovatività di questo metodo sta proprio nel fatto che si è basato su un database di dati reali, a differenza della stragrande maggioranza degli indici che si basano prevalentemente sulla percezione della corruzione[68].

L'esperimento proposto dagli studiosi spagnoli può offrire una serie di vantaggi: rafforzamento della logica preventiva, in quanto il sistema di allerta precoce ha esclusivamente questa finalità; potrebbe costituire

un correttivo molto importante per la policy anticorruzione di tutti i paesi al fine di rendere più effettive le misure e per utilizzare un sistema più sostenibile anche dal punto di vista delle risorse impiegate; considerare la programmazione *machine learning*, *deep learning* nello specifico, come un tipo di IA che se usato nel giusto modo può costituire un serio alleato per la causa dell'anticorruzione.

Operazione Serenada de amor *in Brasile*

L'operazione *Serenada de amor*, esempio di strategia anticorruzione dal basso[69], consiste in un progetto di intelligenza artificiale finalizzato all'analisi della spesa pubblica in Brasile. L'iniziativa è partita nel 2016 dal *data scientist* Irio Musskopf, il quale è stato in grado di fornire le risorse necessarie per sviluppare il sito web che attualmente conta un nutrito gruppo di persone e più di 600 componenti del gruppo Telegram. La realizzazione del progetto è stata possibile attraverso una campagna di auto finanziamento e attraverso la collaborazione con il sito GitHub che è un servizio di hosting per progetti software. Il sito web su cui si basa l'iniziativa è il risultato di un progetto tecnologico che ha cercato di utilizzare l'intelligenza artificiale, *machine learning* in particolare, per controllare i conti pubblici dei politici brasiliani, con l'obiettivo di favorire un vero e proprio monitoraggio diffuso. Il sito *Serenada de amor*[70] è stato sviluppato con dati pubblici aperti, consentendo pertanto a qualsiasi cittadino di esaminare l'impiego della quota dedicata all'esercizio delle attività parlamentari (CEAP) dei deputati federali e dei senatori brasiliani relativamente al rimborso di varie spese, come il vitto, trasporto, alloggio e attività educative e culturali.

La pagina web ha sviluppato un robot open source chiamato *Rosie*, che analizza le spese rimborsate ai deputati e senatori, individuando sospetti e favorendo il controllo sociale della spesa pubblica. Le tecniche usate si basano sull'apprendimento automatico che consente di individuare i rimborsi anomali nel CEAP, i cui risultati vengono successivamente pubblicati sui social media in modo che i cittadini possano visualizzarli, indagare, interrogarli e persino segnalarli. Al fine di consentire ai cittadini la comprensione delle informazioni generate da *Rosie*, il sito ha creato un apposito software *Jarbas*, che facilita la verifica delle informazioni relative al rimborso delle spese dei parlamentari.

Sono passati un po' di anni dallo sviluppo di questa esperienza e, nonostante l'impatto innovativo e la natura *bottom-up* del progetto, emergono alcuni elementi che portano alla luce la difficoltà di utilizzo diffuso di questo sistema. Le caratteristiche che quest'approccio porta con sé evidenziano che, nonostante l'ausilio dell'IA, rimane centrale il ruolo delle persone nel verificare i sospetti rilevati dai bot. Proprio per questo motivo, la partecipazione delle persone è minacciata e disincentivata, in questo tipo di iniziative, da alcune conseguenze problematiche che potrebbero tradursi in forme ritorsive vere e proprie o potrebbero comportare citazioni in giudizio.

ProZorro *in Ucraina*

La piattaforma di *e-procurement ProZorro*, basata sull'utilizzo di IA e di *machine learning*, è stata sviluppata da attivisti e volontari ed è entrata in vigore nel 2015, quando in Ucraina si avvertiva una forte necessità di varare una serie di riforme anticorruzione[71]. Il sistema che sta alla base di *ProZorro* è caratterizzato dal fatto che permette di condurre gare d'appalto in condizioni di totale apertura in tutte le fasi dell'acquisto e offre le stesse condizioni di partecipazione agli appalti pubblici. La finalità del progetto è infatti quella di sollecitare il coinvolgimento di nuovi fornitori che non hanno mai partecipato alle gare pubbliche e quindi aumentare la concorrenza nel settore. Per giunta, si consente un controllo vero e proprio sull'utilizzo dei fondi in modo trasparente ed efficiente.

Gli specialisti di *ProZorro* hanno introdotto un sistema elettronico di appalti pubblici basato su un modello multipiattaforma, che ha consentito loro di utilizzare i servizi di tante piattaforme elettroniche commerciali già attive in Ucraina: il portale prozorro.gov.ua scambia in modo automatico le informazioni e i documenti con le altre piattaforme elettroniche. Nella piattaforma principale sono riportate le caratteristiche degli appalti pubblici ripartiti per dimensione, in particolare: sottosoglia, sopra soglia, soglie speciali e le procedure per tre tipi principali di appalto pubblico (gara d'appalto aperta, gara d'appalto a partecipazione limitata, dialogo competitivo) e una aggiuntiva (appalto a procedura negoziata).

Gli appalti pubblici attraverso *ProZorro* agiscono come una sorta di meccanismo di controllo statale sulla regolazione delle condizioni di mercato, rappresentando di conseguenza un valido strumento per prevenire la corruzione in questo settore.

Le prime analisi mostravano l'esistenza di una tendenza negativa della concorrenza e la riduzione dell'ammontare dei risparmi nei fondi pubblici. *ProZorro* ha diffuso inoltre tutte le informazioni sugli appalti governativi, oltre a creare tanti dati standardizzati utili sia per il controllo che per l'analisi.

Da alcune stime risulta che il sistema abbia ridotto in modo notevole la corruzione: attraverso aste online trasparenti e controllo pubblico, ha consentito allo Stato di risparmiare parecchi fondi pubblici[72].

ProZorro dimostra insomma che big data e open data possono essere considerati come mezzi seri per

monitorare e prevenire la corruzione. Ovviamente, come per ogni potenziale strumento IA nel campo dell'anticorruzione, anche questo sistema dev'essere integrato in un sistema di controllo più ampio, collegato con la legislazione in materia e con un ruolo determinate dell'autorità/agenzia anticorruzione.

4. Quali sfide e rischi ne derivano in termini di legalità e partecipazione?

Nelle pagine precedenti si è cercato di considerare come e in quali casi l'intelligenza artificiale potrebbe essere utile per perfezionare e semplificare (misure e risorse) il sistema della prevenzione della corruzione. Tralasciando le esperienze brevemente descritte, si vuole circoscrivere il raggio della riflessione alla pubblica amministrazione, al fine di considerare il probabile impatto dell'IA sulla legalità[73] e la partecipazione per quanto riguarda lo sviluppo dei Ptpct.

Relativamente alla cd. "legalità algoritmica" e alla crisi di legittimità dello Stato amministrativo automatizzato[74] si è già discusso ampiamente, soprattutto in relazione al tema della decisione amministrativa e della discrezionalità, alle prime valutazioni e sentenze del giudice amministrativo in materia[75]; alla compatibilità dell'algoritmo, a date condizioni[76], con l'attività e l'organizzazione della pubblica amministrazione.

Nel caso in cui il processo che porta all'adozione dei piani di prevenzione fosse interamente governato dall'IA, l'attuale iter di predisposizione dovrebbe essere completamente rielaborato in virtù del venir meno di importanti elementi costitutivi. Nelle fasi del processo di gestione del rischio, come già affermato, è determinante il ruolo del funzionario umano, soprattutto per motivi insiti nella legalità amministrativa. Come noto, il piano è un documento di natura programmatoria determinato da caratteristiche, garanzie e responsabilità simili ad un procedimento amministrativo[77]: motivazione delle scelte adottate; ruolo di coordinamento del processo di gestione del rischio affidato a un responsabile (Rpct); l'ascolto e la partecipazione degli *stakeholder*.

Nonostante la l. 6 novembre 2012, n. 190 non sancisca espressamente l'obbligo della motivazione delle misure organizzative assunte, ciò è deducibile indirettamente all'interno dei piani nazionali anticorruzione dell'ANAC e direttamente nell'allegato 1 del PNA del 2019[78].

Ogni decisione che viene presa in merito alle singole fasi del Ptpct dev'essere motivata al fine di garantire la massima trasparenza, nonché per rendere ragione del perché sono state preferite alcune soluzioni rispetto ad altre e con quali vantaggi. In particolare, le scelte che necessitano della motivazione sono le seguenti: approccio valutativo, rilevazione dei dati e delle informazioni, misurazione applicata e le modalità di campionamento utilizzate.

Nell'analisi del rischio un fattore determinante è la scelta dell'approccio valutativo. I criteri di valutazione che vengono scelti debbono essere valutati e motivati per ridurre l'autoreferenzialità della scelta e per fornire le conseguenti evidenze a supporto. Dato che si tratta di un documento di programmazione, un'altra motivazione che dev'essere resa è quella legata alla scelta del tipo di campionamento usato per il monitoraggio del piano, che può essere di tipo statistico o ragionato. Un'ultima motivazione è quella della cd. "misurazione applicata" relativa alla rilevazione e alla valutazione del livello di esposizione al rischio, consistente in una valutazione complessiva basata sui singoli indicatori.

La completa assunzione dei compiti da parte della macchina eliminerebbe inoltre il ruolo di coordinatore del processo di predisposizione del piano affidato al responsabile (Rpct). Tale aspetto contribuirebbe a due conseguenze negative: mancanza di un soggetto sul quale far ricadere eventuali responsabilità legate alla procedura; contrasto con i poteri e le funzioni attribuite al Rpct dalla legislazione vigente. Si delinea quindi una vera e propria incompatibilità tra la totale decisione automatizzata e il Rpct, almeno all'interno del processo di gestione del rischio.

Un'altra questione molto importante è quella legata alle probabili discriminazioni scaturite dalle misure di prevenzione, qualora venissero decise completamente dall'algoritmo. Potrebbero essere adottate misure caratterizzate da una profilazione di criteri stereotipati e discriminatori. Ciò potrebbe accadere a causa di problemi di apprendimento, ovvero: «dalla gestione non corretta dei dati presi in considerazione nella fase in cui il software elabora i propri modelli decisori»[79]. L'approccio di genere nei piani è molto importante per valutare le variabili biologiche, ambientali e sociali, al fine di migliorare l'appropriatezza degli interventi di prevenzione e far sì che la dimensione di genere contribuisca a evitare stereotipi e a definire strategie volte ad evitare disuguaglianze[80]. Questo pericolo potrebbe essere evitato attraverso la preliminare programmazione se si trattasse dell'IA *rule-based programming*; invece, si riscontrerebbero serie difficoltà di fronte alla tipologia *machine learning*.

Alla luce di ciò, si pone dunque un serio problema di disparità di trattamento dei destinatari delle misure decise dall'IA, in chiaro contrasto con gli artt. 3 e 97 Cost. e nel caso di discriminazione di genere anche degli artt. 7 e 35 del d.lgs. n. 165/2001.

Un ultimo elemento è quello della protezione dei dati ai sensi del Regolamento (UE) 2016/679. Infatti,

uno dei primi step dell'iter di approvazione dei Ptpct consiste in un'ampia raccolta di dati (fonti interne ed esterne), che possono poi confluire in banche dati digitali. Alcuni di questi dati, tuttavia, sono soggettivi e ricavati dagli *stakeholder* relativi alla percezione che questi hanno del fenomeno corruttivo e che per questo motivo rappresentano dati personali.

Anche in questo caso, bisogna formulare due distinte ipotesi: 1) utilizzo limitato dell'IA *rule-based programming*, dove il programmatore umano inserisce i dati nel rispetto della normativa GDPR; 2) se, invece, l'elemento umano fosse esterno, l'algoritmo non sarebbe quasi certamente capace di rispettare questi princìpi.

L'applicazione estesa dell'IA al sistema appena illustrato comporterebbe: a) l'impossibilità di esprimere le motivazioni delle scelte determinate dalle procedure automatizzate; b) scarsa, se non assente, *explainability* del processo decisionale, ovvero come si arriva dall'input all'output[81]; c) il difficile rapporto tra il processo di elaborazione automatizzata delle misure di prevenzione e il rischio che le misure possano essere discriminatorie nei confronti dei funzionari e delle funzionarie; d) le questioni problematiche legate alla protezione della privacy e dei dati adoperati nel processo di gestione del rischio.

Se si trattasse di ricorrere alle tecniche IA limitatamente ad alcuni elementi, ciò permetterebbe di mantenere salvo l'attuale impianto dell'approvazione dei Ptpct e, come detto, favorirebbe un significativo efficientamento sia della gestione dei dati grazie alle tecniche *blockchain* che della bontà degli indicatori di rischio adoperati attraverso la definizione di tecniche IA e di *machine learning*.

Viceversa, se il ruolo cruciale e onnipresente del funzionario (specie del Rpct) venisse soppiantato da forme di IA capaci di fare a meno del contributo umano, due sarebbero le possibili conseguenze: 1) si dovrebbe accantonare il sistema finora adottato e varare un'adeguata regolamentazione, nella quale l'intervento umano sarebbe esterno al processo ma che potrebbe garantire il controllo *ex-post* sulle misure; 2) tale ipotesi non dovrebbe essere ritenuta praticabile in quanto verrebbero meno delle garanzie legali molto importanti.

4.1. Segue. Prevenzione della corruzione e partecipazione

Nel framework italiano di prevenzione della corruzione la partecipazione assume un ruolo molto importante ed è estesa a tanti soggetti e fasi, sia interni che esterni alla pubblica amministrazione.

La logica preventiva infatti confida nel personale dell'amministrazione sia per la promozione e il rispetto di doveri e misure che per il contributo in fase di formazione e aggiornamento dei Ptpct e dei codici di comportamento. I piani di prevenzione vedono un diretto coinvolgimento di vari soggetti interni alla struttura e degli *stakeholder* sia interni che esterni. Infatti, oltre al Responsabile sono coinvolti nel processo di gestione del rischio tanti altri uffici, organismi, la dirigenza e il personale dipendente. Oltre all'organigramma vero e proprio, vi sono gli *stakeholder* ovvero quegli altri uffici che vengono informati e invitati ad esprimere pareri sulla bozza di piano che poi verrà adottata. È previsto anche un contributo partecipativo dei cittadini e delle organizzazioni portatrici di interessi, che possono essere consultati e a loro volta possono far pervenire le proprie osservazioni e suggerimenti nella fase di aggiornamento[82]. Ciò si concretizza con l'invio delle proposte attraverso un apposito modulo allegato all'indirizzo e-mail del responsabile, tramite pec o in una sezione dedicata del portale web dell'amministrazione[83].

Premesso ciò, anche l'elemento partecipativo verrebbe dunque notevolmente compromesso nel caso in cui gli algoritmi venissero utilizzati in modo estensivo nel processo di adozione dei Ptpct. Se la scelta delle misure fosse completamente scaturita dalle procedure automatizzate, il contributo dei soggetti interni ed esterni non avrebbe senso e quindi verrebbe meno un pilastro dell'attuale sistema *bottom-up* di co-definizione delle misure, nel quale anche i soggetti esterni all'amministrazione vengono coinvolti in una logica di cittadinanza amministrativa partecipe e attenta alla buona amministrazione[84].

L'ipotetico sistema di definizione delle misure basato esclusivamente sull'IA si pone inoltre come paradossale rispetto alla maggioranza dei casi in cui, l'utilizzo estensivo delle ICT, rideterminerebbe in positivo il ruolo tra cittadino e amministrazione sul profilo della partecipazione ai processi decisionali[85]. Un simile impianto, tra l'altro, si porrebbe in chiaro contrasto con le raccomandazioni internazionali in tema di anticorruzione e integrità pubblica (Ocse su tutti[86]), dove alla partecipazione viene conferito un valore di primaria importanza.

Le ripercussioni escludenti in tema di partecipazione sarebbero estese anche alla fase di adozione e revisione dei codici di comportamento delle singole amministrazioni: i doveri integrativi delle PA devono essere adottati sulla base delle evidenze e misure risultanti dal processo di *risk assessment* dei Ptpct; inoltre l'art. 54, co. 5 del d.lgs. n. 165/2001 prevede una "procedura aperta alla partecipazione" per l'adozione e la revisione dei codici di amministrazione. Di conse-

guenza, le regole di condotta dei codici, che appunto sono collegate con i piani, sarebbero prive del momento partecipativo iniziale dei soggetti interni ed esterni all'amministrazione, le cui procedure di presentazione delle istanze sono simili a quelle dei Ptpct.

Il contesto appena ipotizzato, nel quale l'IA escluderebbe la partecipazione interna ed esterna, si pone inoltre in controtendenza con le esperienze di controllo e prevenzione della corruzione dal basso, come i casi sopra descritti[87]. In effetti, in un clima di crescente coinvolgimento dei cittadini alla causa preventiva, in alcuni casi in forma autonoma e in altri attraverso collaborazioni sinergiche con le istituzioni, si andrebbe a compiere un significativo passo indietro. Il sistema di prevenzione della corruzione italiano, indicato da tanti come un *framework* ideale anche per il fattore partecipativo e l'attuazione della politica dal basso, rinuncerebbe quindi ad un suo fattore costitutivo. Di conseguenza, di fronte ad uno scenario così configurato, sorge il dubbio se abbia ancora senso continuare a parlare del modello anticorruzione attuale o se invece, in base alle condizioni ipotizzate, sia piuttosto il caso di parlare di abrogazione della legge 190/2012 e di sollecitare il Parlamento italiano a legiferare in merito ad un nuovo impianto dove il processo di definizione delle misure sarà governato dagli algoritmi e non più dall'essere umano.

5. Riflessioni conclusive

Sebbene nelle pagine precedenti si possa scorgere un certo pessimismo circa la fattibilità di impiego dell'IA nel processo di adozione dei Ptpct e nell'organizzazione preventiva *tout-court*, in realtà si tratta solo di ragionare su alcune questioni controverse ed eventuali cautele da dover adottare[88].

L'indubbio apporto in termini di efficientamento, risparmio di risorse e di perfezionamento di alcuni strumenti induce senz'altro a sperare che tali tecniche vengano utilizzate nel campo dell'anticorruzione. Tuttavia, però, bisogna riconoscere che l'intervento umano nel processo di gestione del rischio e in altri campi non può essere eliminato o marginalizzato a mero controllo successivo all'adozione delle misure. L'attuale impianto infatti è stato concepito dal legislatore del 2012 come un vero e proprio investimento sul personale e sulla capacità delle amministrazioni di implementare la policy in modo proattivo e partecipato. Si tratta dunque di effettuare un bilanciamento tra i rischi e i benefici che si ripercuoterebbero sulla legalità, l'imparzialità e buon andamento. Detto in altre parole, non possiamo solo considerare gli eventuali vantaggi per quanto concerne una maggiore efficienza ed economicità del processo, bensì bisogna avere la consapevolezza di cosa potremmo perdere anche in termini di deficit legale.

La proposta che emerge da questo contributo è quella di auspicare un sistema che si possa avvalere dell'IA e non che, viceversa, il contributo umano venga rimpiazzato dagli algoritmi. Appare alquanto sostenibile uno scenario in cui il funzionario umano, preservando una certa "meta-autonomia"[89], possa continuare a svolgere un ruolo determinante nel campo dei piani anticorruzione, ma utilizzando strumenti e tecniche IA in grado di facilitare i vari processi, perfezionare la gestione dei dati e fornire indici e segnali di allarme più precisi ed attendibili per le successive scelte da prendere.

Stesse considerazioni sono valide per quegli ambiti che non fanno parte del sistema della prevenzione della corruzione, ma che assurgono a presidio dell'integrità della PA. In questi casi, risulterà necessario prevedere meccanismi e garanzie che possano scongiurare eventuali discriminazioni prodotte dalle procedure automatizzate e a far sì che il trattamento dei tanti dati operati dall'IA avvenga nel rispetto della normativa di privacy e protezione dei dati personali.

In conclusione, al di là degli scenari prefigurati, sarà fondamentale la regolamentazione dell'IA in tutto il settore pubblico e soltanto dopo le pubbliche amministrazioni potranno essere in grado di sistematizzare l'impiego dell'intelligenza artificiale in ogni ambito e nel sistema della prevenzione della corruzione in particolare.

Le difficoltà, come detto, sono molte ma occorre affrontarle in modo organico senza pregiudizi e senza sottovalutazioni, altrimenti le questioni attuali potrebbero moltiplicarsi anziché diminuire. L'IA è infatti un mezzo creato per risolvere problemi precedentemente irrisolti, non per risolvere problemi che si devono prima creare.

Note

[1] A. Petheram, W. Pasquarelli, R. Stirling, *The Next Generation of Anti-Corruption Tools: Big Data, Open Data & Artificial Intelligence*, in "Oxford Insights", 2019; N. Köbis, C. Starke, I. Rahwan, *Artificial Intelligence as an Anti-Corruption Tool. Potentials and Pitfalls for Top-down and Bottom-up Approaches*, in "arXiv.org", 2021; M.S.M. Lima, D. Delen, *Predicting and explaining corruption across countries: A machine learning approach*, in "Government information quarterly", vol. 37, 2020, n. 1; N. Kossow, *Digital anti-corruption: hopes and challenges*, in A. Mungiu-Pippidi, P. Heywood (eds.), "A Research Agenda for Studies of Corruption", Edward Elgar Publishing, 2020; P. Aarvik, *Artificial Intelligence - A promising anti-corruption tool in development settings?* U4: Anti-Corruption Resource Center, 2019; F. Odilla, *Avoiding minority reports: using AI responsibly in anti-corruption*, in "Corruption, Justice and Legitimacy Program", 2022; V. Sharma, *Can artificial intelligence stop*

corruption in its tracks?, in "World Bank Blog", 2019; I. Adam, M. Fazekas, *Are emerging technologies helping win the fight against corruption? A review of the state of evidence*, in "Information Economics and Policy", vol. 57, 2021; I. Villamil, J. Kertész, J. Wachs, *Computational Approaches to the Study of Corruption*, in "arXiv.org", 2022; K. Scheer, T. Rable, N. Köbis, *AI-Based Software as Anti-Corruption Agent and Its Influence on Employees' Likelihood of Whistleblowing*, in S. Taneja (eds.), "Academy of Management. Proceedings", vol. 1, Briarcliff Manor, 2022.

[2]OECD, *Analytics for Integrity. Data driven approaches for enhancing corruption and fraud risk assessments*, 2019.

[3]Tale termine è rinvenibile in I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in "Istituzioni del Federalismo", 2019, n. 3, p. 645.

[4]Sul sistema italiano di prevenzione della corruzione si vedano R. Cantone, *Il sistema della prevenzione della corruzione*, Giappichelli, 2020; F. Merloni, *Corruption and Public Administration. The Italian Case in a Comparative Perspective*, Routledge, 2018; E. Carloni, M. Gnaldi, *Understanding and Fighting Corruption in Europe. From Repression to Prevention*, Springer, 2021; R. Cantone, E. Carloni, *La prevenzione della corruzione e la sua Autorità*, in "Diritto Pubblico", 2017, n. 3, pp. 903-944.

[5]Si veda in tal senso S. Battini, V. Lostorto, *Il ruolo della formazione nella politica di prevenzione della corruzione*, in L. Donato (a cura di), "Gli appalti pubblici tra istanze di semplificazione e normativa anticorruzione. Alla ricerca di un equilibrio tra legalità ed efficienza", serie Quaderni di Ricerca Giuridica, 2020, n. 89, pp. 225-242.

[6]OECD, *Recommendation of the Council on Public Integrity*, 2017.

[7]In generale sull'IA si vedano P. Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 2020; C. Bartneck, C. Lütge, *What Is AI?* in C. Bartneck, C. Lütge, A. Wagner, S.W. An (eds.), "Introduction to Ethics in Robotics and AI", Springer, 2021; K. Crawford, *Né intelligente né artificiale. Il lato oscuro della IA*, il Mulino, 2021.

[8]N. Heath, *What is artificial general intelligence?*, August 22, 2018.

[9]M. Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*, Farrar Straus & Giroux, 2019.

[10]Sulla relazione tra *machine learning* e decisione amministrativa si veda C. Coglianese, D. Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, Faculty Scholarship at Penn Carey Law, 2017.

[11]Una rete neurale artificiale è in grado di gestire astrazioni sofisticate, utilizzando i suoi strati nascosti per apprendere la presenza di caratteristiche astratte contenute nei dati. Una semplice rete neurale è organizzata in diversi strati di neuroni.

[12]Così C. Casonato, *Giustizia e intelligenza artificiale: considerazioni introduttive*, in "BioLaw Journal", 2021, n. 2, pp. 359-365.

[13]Un esempio è il cd. *Rule-based machine learning* (RBML), consistente in un metodo di apprendimento automatico che identifica, apprende o fa evolvere "regole" da archiviare, manipolare o applicare. Sempre sul tema, si vedano R. El Hamdani, M. Mustapha, D. Restrepo Amariles et al., *A combined rule-based and machine learning approach for automated GDPR compliance checking*, in "ICAIL '21: Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law", 2021, pp. 40-49; Ö. Uzuner, X. Zhang, T. Sibanda, *Machine Learning and Rule-based Approaches to Assertion Classification*, in "Journal of the American Medical Informatics Association", vol. 16, 2009, n. 1, pp. 109-115.

[14]Sul legame big data-intelligenza artificiale per la lotta alla corruzione si rinvia a European Parliament, *Workshop on: Use of big data and AI in fighting corruption and misuse of public funds - good practice, ways forward and how to integrate new technology into contemporary control framework*, 2021.

[15]Così J.M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in "Public Law Research paper in the age of big data", 2017, p. 6.

[16]Cfr. A. Le Sueur, *Robot Government: Automated Decision-making and its Implications for Parliament*, in A. Horn, A. Le Sueur (eds.), "Parliament: Legislation and Accountability", Hart Publishing, 2016, p. 18.

[17]Tali obiettivi e azioni sono individuati nel recente documento Ministero dell'Università e della Ricerca, Ministero dello Sviluppo Economico e Ministro per l'Innovazione tecnologica e la Transizione Digitale (a cura di), *Programma strategico. Intelligenza artificiale 2022-24*, 2021.

[18]*Ivi*, p. 10. Con il decreto interministeriale 6 dicembre 2021 è stato istituito un fondo per interventi volti a favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, *blockchain* e *Internet of Things*.

[19]I. Kant, *Metafisica dei costumi*, Laterza, 2009.

[20]S. Kierkegaard, *Aut-aut*, Mondadori, 2016.

[21]Così M. D'Angelosante, *La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in S. Civitarese Matteucci, L. Torchia (a cura di), "A 150 anni dall'unificazione amministrativa italiana. La tecnificazione", vol. IV, La tecnificazione, Firenze University Press, 2016, p. 159 ss.

[22]Consiglio di Stato sez. VI, 8 aprile 2019, n. 2270.

[23]L'applicazione di questa tecnica nella PA dovrebbe incrementare il livello di fiducia, sicurezza e trasparenza, così in The European union blockchain observatory & forum, *Blockchain for Government and Public Services*, 2018.

[24]Secondo l'ANAC le principali fonti sono queste: riguardo alle fonti esterne, l'amministrazione può reperire una molteplicità di dati relativi al contesto culturale, sociale ed economico attraverso la consultazione di banche dati o di studi di diversi soggetti e istituzioni (ISTAT, Università e Centri di ricerca, ecc.). Particolare importanza rivestono i dati giudiziari relativi al tasso di criminalità generale del territorio di riferimento (ad esempio, omicidi, furti nelle abitazioni, scippi e borseggi), alla presenza della criminalità organizzata e/o di fenomeni di infiltrazioni di stampo mafioso nelle istituzioni, nonché più specificamente ai reati contro la pubblica amministrazione (corruzione, concussione, peculato etc.) reperibili attraverso diverse banche dati (ISTAT, Ministero di Giustizia, Corte dei Conti o Corte Suprema di Cassazione). Può essere molto utile inoltre condurre apposite indagini relative agli *stakeholder* di riferimento attraverso questionari online o altre metodologie idonee (es. focus group, interviste etc.). Mentre riguardo alle fonti interne, l'amministrazione può utilizzare interviste con l'organo di indirizzo o con i responsabili delle strutture; segnalazioni ricevute tramite il canale del *whistleblowing* o altre modalità; risultati dall'azione di monitoraggio del Rpct; informazioni raccolte nel corso di incontri e/o attività congiunte con altre amministrazioni che operano nello stesso territorio o settore, in ANAC, *Allegato 1. Indicazioni metodologiche per la gestione dei rischi corruttivi*, 2019, p. 9.

[25]*Ibidem*.

[26]A tal riguardo si veda Future of Life Institute, *Asilomar AI Principles*, 2017 (principles developed in conjunction with the 2017 Asilomar conference); J. Cowls, L. Floridi, *Prolegomena to a White Paper on an Ethical Framework for a Good AI Society*, 2018.

[27]G. Misuraca, C. Van Noordt, *AI Watch - Artificial Intelligence in public services*, Publications Office of the European Union, 2020, JRC120399.

[28]Tale termine si rinviene in E. Carloni, *AI, algoritmi e pubblica amministrazione in Italia*, in "IDP: Revista de Internet, Derecho y Politica", 2019, n. 30; Inoltre, è importante in tal senso TAR Lazio, sez. III bis, 13 settembre 2019, n. 10964, nella quale si afferma che: «Il Collegio è del parere che le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere».

[29]Relativamente al difetto di motivazione e opacità dell'algoritmo, si veda R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in "Rivista trimestrale di diritto amministrativo", 2020, n. 2, pp. 313-317. Sulla decisione amministrativa automatizzata si veda G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica*, in "MediaLaws", 2019, n. 3; R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in "Diritto amministrativo", 2019, n. 4.

[30]Così D.-U. Galetta, J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in "federalismi.it", 2019, n. 3, p. 14.

[31]ANAC, *Pna 2012. Allegato 2: Le aree di rischio*, 2012.

[32]In particolare, al comma 16 dell'art. 1.

[33]In particolare la lett. b) del comma 1 sancisce: «l'utilizzo di strumenti informatici e digitali e, facoltativamente, lo svolgimento in videoconferenza della prova orale, garantendo comunque l'adozione di soluzioni tecniche che ne assicurino la pubblicità, l'identificazione dei partecipanti, la sicurezza delle comunicazioni e la loro tracciabilità, nel rispetto della normativa in materia di protezione dei dati personali e nel limite delle pertinenti risorse disponibili a legislazione vigente».

[34]Si tratta del combinato disposto degli artt. 1, 3, 51 e 97 Cost.

[35]In merito a ciò di veda L. Iannuccilli, A. De Tura (a cura di), *Il principio di buon andamento dell'amministrazione nella giurisprudenza della Corte costituzionale*, in "www.cortecostituzionale.it", 2015.

[36]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[37]In tal merito si veda E.J. Maier, *Advancing Artificial Intelligence and Machine Learning in the U.S. Government Through Improved Public Competitions*, in "arXiv.org", 2021. Sulla relazione tra intelligenza artificiale, apprendimento automatico e discriminazione di genere si evincono spunti interessanti in M.T. Nuseir, B.H. Al Kurdi, M.T. Alshurideh, H.M. Alzoubi, *Gender Discrimination at Workplace: Do Artificial Intelligence (AI) and Machine Learning (ML) Have Opinions About It*, Springer, 2021.

[38]Sulla questione della potenziale discriminazione derivante dall'IA si veda M. Peruzzi, *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in "Labour & Law Issues", 2021, n. 1; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà*, in "BioLaw Journal", 2019, n. 1; I. Valenzi, *Libertà religiosa e intelligenza artificiale: prime considerazioni*, in "Quaderni di diritto e politica ecclesiastica", 2020, n. 2; L. Giacomelli, *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in "BioLaw Journal", 2019, n. 2.

[39]«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. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: 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. 3. 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. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

[40]Sul punto si vedano F. Pizzetti (a cura di), *Intelligenza artificiale e, protezione dei dati personali e regolazione*, Giappichelli, 2018; F. Lorè, *Una intelligenza artificiale più umana, tra etica e privacy*, in "Ciberspazio e diritto: rivista internazionale di informatica giuridica", 2021, n. 1, pp. 165-203; T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in "dpce online", 2022, n. 1, pp. 273-284; C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in "BioLaw Journal", 2019, n. 2, pp. 711-725.

[41]In tal senso A. Pajno, M. Bassini, Gi. De Gregorio et al., *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in "BioLaw Journal", 2019, n. 3, p. 208.

[42]ANAC, *Misurazione territoriale del rischio corruzione e promozione della trasparenza – Progetto PON*, 2020. Alla data di gennaio 2022 sono stati identificati ben 71 indicatori per la misurazione e il contrasto della corruzione, suddivisi in 3 aree tematiche distinte: 1. Indicatori di contesto (49 indicatori articolati in 4 ambiti – Criminalità, Istruzione, Economia e territorio, Capitale Sociale –); 2. Indicatori sugli Appalti (17 indicatori) incentrati sulla banca dati nazionale dei contratti pubblici di ANAC; 3. Indicatori "comunali" relativi ai Comuni sopra 15.000 abitanti (5 indicatori), in *Indici di misurazione della corruzione. Il progetto di Anac, dibattito con Eurispes*, webinar, gennaio 2022.

[43]M. Gnaldi, B. Ponti, *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Franco Angeli, 2018, p. 66.

[44]M. Salles Melo Lima, D. Delen, *Predicting and explaining corruption across countries: A machine learning approach*, in "Government Information Quarterly", vol. 37, 2020, n. 1; F.J. López-Iturriaga, I. Pastor Sanz, *Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces,* Social indicators Research, Springer, 2018, pp. 975-998; L.M.C. Doria, F.F. Doria, P. Figueiredo et al., *A Machine Learning Approach on the Problem of Corruption*, in "International Journal of Advanced Engineering Research and Science", vol. 9, 2022, n. 3.

[45]Sul tema V. Frosini, *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), "Privacy e banche dei dati", il Mulino, 1981.

[46]L'art. 2 specifica che il regolamento si applica: «al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi». Sul tema si rinvia a T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in "dpce online", 2022; T.E. Frosini, *Le sfide attuali del diritto ai dati personali*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), "Dati e algoritmi. Diritto e diritti nella società digitale", il Mulino, 2020; G. Finocchiaro, *XVIII lezione: intelligenza artificiale, privacy e data protection*, in U. Ruffolo (a cura di), "XXVI Lezioni di diritto dell'intelligenza artificiale", Giappichelli, 2021.

[47]Diffusamente sul punto si veda G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018.

[48]L'elaborazione di questi tre modelli si rinviene in N. Köbis, C. Starke, *Artificial Intelligence as an Anti-Corruption Tool. A Conceptual Framework*, 2021, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

[49]Cfr. art. 4, par. 1, n. 1.

[50]Di recente è stato creato un indice di rischio relativo di corruzione in una ricerca finalizzata a valutare l'uso di algoritmi di apprendimento automatico nell'individuazione precoce della corruzione nella pubblica amministrazione, in K.M.S. Munoz, *Inteligencia Artificial para Detectar Corrupción en la Administración Pública Municipal de Colombia*, Documento CEDE-Estudiantes, 2021.

[51]È interessante, in questo senso, uno studio effettuato in due CCIA italiane in D. Galli, G. Giacomelli, G. Valotti, *Misurazione della performance e gestione del rischio: l'utilizzo di indicatori red flag per la prevenzione della corruzione nel settore pubblico*, in "Azienda Pubblica", 2018, n. 2, pp. 147-163.

[52]Per far ciò sono stati indicati i seguenti progetti: favorire lo *smart procurement*; interoperabilità del sistema eProc; processi di dichiarazione e verifica dei requisiti per la partecipazione agli appalti pubblici; aste digitali; CRM evoluto; ricorso a IA e *machine learning*.

[53]*Piano Nazionale di Ripresa e Resilienza*, 2021.

[54]Si segnala una recente analisi molto interessante basata su metodi tradizionali di regressione e metodi di apprendimento automatico in M. Fazekas, S. Sberna, A. Vannucci, *The extra-legal governance of corruption: Tracing the organization of corruption in public procurement*, in "Governance", vol. 35, 2022, n. 4, pp. 1139-1161.

[55]Su indicatori di rischio nel campo del *public procurement* si vedano M. Fazekas, I.J. Toth, L.P. King, *An Objective Corruption Risk Index Using Public Procurement Data*, in "European Journal on Criminal Policy and Research", 2016, n. 22, pp. 369-397; M. Fazekas, G. Kocsis, *Uncovering high-level corruption: Crossnational objective corruption risk indicators using public procurement data*, in "British Journal of Political Science", vol. 50, 2020, n. 1, pp. 155-164.

[56]Così A. Sanchez-Graells, *Can artificial intelligence bring corruption in public procurement to an end?*, in "University of Bristol Law School Blog", 2021.

[57]Sul sito di Cineca.it il *text mining* viene definito come una tecnica di intelligenza artificiale che utilizza l'elaborazione del linguaggio naturale per trasformare il testo libero, non strutturato in dati strutturati e normalizzati.

[58]Tali ipotesi sono sostenute in K. Rabuzin, N. Modrušan, *Prediction of Public Procurement Corruption Indices using Machine Learning Methods*, in J.L.G. Dietz, D. Aveiro, J. Filipe (eds.), "Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019)", Scitepress, 2019, pp. 333-340.

[59]Così P. Aarvik, *Blockchain as an anticorruption tool. Case examples and introduction to the technology*, in "U4 Issue", 2020.

[60]Tale termine si deve a E. Carloni, *Il paradigma trasparenza. Amministrazioni, informazioni, democrazia*, il Mulino, 2022, p. 292.

[61]Al comma 5 dell'art. 1 della l. n. 179/2017 è infatti sancito che: «le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione».

[62]Garante per la protezione dei dati personali, *Newsletter n. 488 dell'11 maggio 2022*.

[63]Tale proposta è presente in A.E.B. Tomaz, J.C. Do Nascimiento, J.N. De Souza, *Blockchain-based whistleblowing service to solve the problem of journalistic conflict of interest*, in "Annals of Telecommunications", vol. 77, 2022, n. 1-2, pp. 101-118.

[64]In questo senso si veda F. Odilla, *Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology*, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

[65]Una raccolta di diverse esperienza si trova in United Nations ESCAP, *Artificial intelligence in the Delivery of Public Services. Report*, 2019.

[66]Gli studiosi hanno scelto di non menzionare i casi più soggetti a corruzione per evitare polemiche.

[67]F.J. López-Iturriaga, I. Pastor Sanz, *Predicting Public Corruption with Neural Networks*, cit.

[68]Relativamente al limite degli indicatori di percezione, alcuni studiosi hanno proposto di basarli sugli *hard data* di fonte amministrativa in B. Ponti, *Oltre la percezione: concretizzare le potenzialità conoscitive degli indicatori basati sull'elaborazione degli hard data di fonte amministrativa*, in M. Gnaldi, B. Ponti (a cura di), "Misurare la corruzione oggi", cit., pp. 47-58.

[69]Vantaggi e problemi derivanti da questo tipo di iniziative, in particolare dell'operazione *Serenada de amor* si riscontrano in F. Odilla, *Citizens and their bots that sniff corruption: Using digital media to expose politicians who misuse public money*, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

[70]Il nome del sito è stato ispirato dal caso Toblerone, che si riferisce all'episodio in cui la popolazione svedese ha chiesto le dimissioni di un ministro per l'acquisto di una tavoletta di cioccolato Toblerone e altre spese personali con la carta aziendale.

[71]Sulle riforme anticorruzione successive al 2014 si veda R. Nizhnikau, *Love the Tender: ProZorro and Anti-Corruption Reforms after the Euromaidan Revolution*, in "Problems of Post-Communism", vol. 69, 2022, n. 2.

[72]Su alcune stime prodotte sull'utilizzo di *ProZorro* si veda A. Kovalchuk, C. Kenny, M. Snyder, *Examining the Impact of E-Procurement in Ukraine*, Center for Global Development Working Paper 511, 2019.

[73]In merito alla relazione tra legalità e decisioni amministrative si rinvia a S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in "Diritto Pubblico", 2019, n. 1.

[74]In merito a ciò si rinvia a R. Calo, D.K. Citron, *The automated administrative law: a crisis of legitimacy*, in "Emory Law Journal", vol. 70, 2021, n. 4, pp. 799-845.

[75]R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in "Diritto amministrativo", 2019, n. 4, pp. 773-792; G. Pesce, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, 2020; G. Marchianò, *La legalità algoritmica nella giurisprudenza amministrativa*, in "Il diritto dell'economia", 2020, n. 3, pp. 229-258; P. Falletta, *Alla ricerca di un paradigma giuridico della decisione amministrativa algoritmica*, in "Amministrazione in cammino", marzo 2022.

[76]Emblematica di ciò è la sentenza TAR. Lazio, sez. III bis, 13 settembre 2019, n. 10964.

[77]All'interno dell'Allegato 1 del PNA 2019 recante "Indicazioni metodologiche per la gestione dei rischi corruttivi", l'ANAC rileva differenze e analogie tra il processo che porta all'adozione di un piano e un procedimento amministrativo vero e proprio, nel quale si afferma che: «Un processo può essere definito come una sequenza di attività interrelate ed interagenti che trasformano delle risorse in un output destinato ad un soggetto interno o esterno all'amministrazione (utente). Si tratta di un concetto organizzativo che – ai fini dell'analisi

del rischio – ha il vantaggio di essere più flessibile, gestibile, completo e concreto nella descrizione delle attività rispetto al procedimento amministrativo».

[78]Nel quale si legge che l'allegato dev'essere considerato come: «l'unico documento metodologico da seguire nella predisposizione dei Piani triennali della prevenzione della corruzione e della trasparenza (Ptpct) per la parte relativa alla gestione del rischio corruttivo».

[79]Così F. Donati, *Intelligenza artificiale e giustizia*, in "Rivista AIC", 2020, n. 1, p. 422.

[80]Tale concetto è centrale in Ministero della Salute - Direzione Generale della Prevenzione Sanitaria, *Piano Nazionale della prevenzione 2020-2025*.

[81]Sulla relazione input-output e IA si veda su tutti F. Pasquale, *Black box society. The secret algorithms that control money and information*, Harvard University Press, 2015.

[82]Anche in questo caso vi sono chiare similitudini con la disciplina sul procedimento amministrativo: partecipazione al procedimento (art. 7 e s., l. 7 agosto 1990, n. 241), diritto di accesso dei partecipi agli atti, di presentare memorie e documenti (art. 10, l. 7 agosto 1990, n. 241).

[83]Per es. per l'invio delle proposte per l'ospedale policlinico San Martino del SSR Liguria viene dato questo indirizzo: responsabile.trasparenza@hsanmartino.it; il Rpct dell'Agcom fornisce questo indirizzo mail: agcom@cert.agcom.it; Per la revisione del codice di comportamento interno, il comune di Palermo ha indicato il seguente indirizzo mail: anticorruzione@comune.palermo.it.

[84]Su cittadinanza amministrativa e buona amministrazione A. Bartolini, A. Pioggia, *Le cittadinanze amministrative, percorsi e prospettive dell'amministrazione tra diritti e doveri a 150 anni dalle leggi di unificazione amministrativa*, in L. Ferrara, D. Sorace (a cura di), "A 150 anni dall'unificazione amministrativa italiana", Firenze University Press, 2016, pp. 9-56.

[85]Si veda in tal senso C. Benetazzo, *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, in "federalismi.it", 2020, n. 16.

[86]Si veda la sezione 13 "Partecipazione" di OECD, *Oecd Public Integrity Handbook*, in "Oecd-ilibrary.org", 2020.

[87]In merito ai potenziali rischi derivanti dall'impiego top-down delle tecniche di intelligenza artificiale si veda N. Köbis, C. Starke, I. Rahwan, *The promise and perils of using artificial intelligence to fight corruption*, in "Nature Machine Intelligence", 2022, n. 4, pp. 418-424.

[88]Anche l'attuale proposta Europa dell'*AI Act* afferma che: «il presente regolamento non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche», in *Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica di alcuni atti legislativi dell'Unione*, COM/2021/206 final, del 21 aprile 2021, p. 30.

[89]Concetto elaborato in L. Floridi, J. Cowls, M. Beltrametti et al., *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in "Minds and Machines", 2018, n. 28, pp. 689-707.

* * *

Legality, algorithms and corruption: can AI techniques be used *in* and *for* the corruption prevention system?

Abstract: The article aims to consider what could be the potential opportunities and risks related to the use of artificial intelligence (AI) techniques in the Italian system of corruption prevention. In particular, it considers the risk management process, as a crucial moment for the adoption of administrative measures for the corruption prevention. The use of AI techniques could improve these phases, speed up the procedure and guarantee greater impartiality in the choice of measures. At the same time, however, the adoption of partial or total AI techniques would bring with it both certain complicated elements and a significant downsizing of the current system. An additional consideration is directed to those areas or instruments that, although not to be considered as strictly internal to the prevention system, could contribute to the preventive cause itself. The final section discusses the problematic aspects that the application of AI in the field of prevention could entail in terms of participation and legality.

Keywords: Artificial intelligence – Corruption prevention – Legality – Participation

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0090
Articolo sottoposto a peer review

Gli algoritmi dell'amministrazione pubblica e l'amministrazione pubblica degli algoritmi

Matteo Palma

Nella prima parte del contributo, dopo aver velocemente illustrato il ruolo del diritto amministrativo nella gestione della complessità sociale, si esaminano l'uso degli algoritmi all'interno delle amministrazioni pubbliche, le problematiche che questi hanno fatto emergere e le soluzioni che letteratura e giurisprudenza hanno offerto. In un secondo momento, invece, per superare il binarismo tra accettazione e rifiuto della digitalizzazione dei procedimenti amministrativi si affronta il tema in un'ottica più ampia, quella, appunto, "dell'amministrazione pubblica degli algoritmi". In questa prospettiva si esamina l'opportunità di interpretare alcuni istituti del Codice dell'amministrazione digitale, come il riuso del software, quali strumenti di coordinamento informatico, per sviluppare la digitalizzazione dell'amministrazione pubblica contemperando le esigenze di differenziazione, da una parte, e preservando la riuscita della transizione digitale, dall'altra.

Datizzazione – Algoritmo pubblico – Codice sorgente – Accesso documentale – CAD – Riuso software – Coordinamento amministrativo

Sommario: *1. Introduzione: la funzione ordinante del diritto amministrativo – 2. L'impiego di ICTs nella pubblica amministrazione: i problemi e le tutele procedimentali – 3. Alcune criticità sistemiche dell'impiego di ICTs nella pubblica amministrazione – 4. Il riuso del software come strumento di governo delle ICTs nell'amministrazione pubblica – 5. (segue) Le potenzialità residue del riuso del software – 6. Considerazioni conclusive*

1. Introduzione: la funzione ordinante del diritto amministrativo

Il fenomeno della "datizzazione"[1] nella sua trasversalità ha recentemente intercettato anche l'attenzione della dottrina amministrativistica. Il progressivo e generale innalzamento dei livelli di sviluppo tecnologico, alla base di tale fenomeno, consente di rappresentare in linguaggio numerico sempre più informazioni provenienti dall'osservazione della realtà. La società intera, nelle sue soggettività e nelle sue interazioni, si presta a divenire un giacimento di informazioni[2] utili ad elaborare migliori soluzioni ai bisogni sociali ma anche, come taluni ravvisano, preziose per chi promuove politiche di controllo sociale. Mediante l'addestramento sui big data, infatti, i sistemi di intelligenza artificiale si rivelano in grado di evidenziare, con minori o maggiori margini di errore, caratteri ricorsivi nel comportamento degli individui e dei gruppi, sulla base dei quali si ritiene possibile prospettare e guidare futuri comportamenti sociali[3].

Su un piano distinto ma attiguo si muove invece il diritto[4] a cui la tradizione giuridica degli Stati moderni liberaldemocratici ha affidato il ruolo di garantire la convivenza tra gli individui riconoscendone i diritti e regolandone le libertà[5]. In questo solco, dunque, si muove il diritto amministrativo, il quale avrebbe la capacità di «promuovere, rispetto alle interazioni tra amministrazioni e amministrati, una razionalità allo

M. Palma è dottorando in Diritto amministrativo presso il Dipartimento di diritto pubblico, italiano e sovranazionale dell'Università degli Studi di Milano. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

stesso tempo strumentale e comunicativa»[6]. La prima si riferisce alla necessità dell'amministrazione di giustificare i fini e i mezzi del suo agire rispetto ai compiti assegnati dalla normativa superiore[7]; essa trova prime, ma non uniche, espressioni nei principi di imparzialità e trasparenza dell'azione amministrativa, positivizzati nell'art. 1 l. 7 agosto 1990, n. 241 e poi ulteriormente declinati nell'obbligo di motivazione e nell'accesso documentale, rispettivamente agli artt. 3 e 22 l. 241/1990. La seconda, invece, è quella sottesa alla procedimentalizzazione dell'attività amministrativa e agli istituti di partecipazione procedimentale che consentono lo «scambio ragionato degli argomenti tra amministrazioni e destinatari dell'azione amministrativa»[8]. Entrambe le razionalità devono essere compresenti perché il diritto amministrativo possa operare come fattore ordinante della comunità politica, da un lato, e, dall'altro, possa legittimare la persistenza di un potere amministrativo in sistemi giuridici sempre più complessi, articolati e debordanti dallo Stato-nazione[9].

Da questa prospettiva, dunque, si può esaminare l'impiego di ICTs che impiegano algoritmi, sistemi di intelligenza artificiale, cloud, etc. nell'azione amministrativa per svolgere alcune considerazioni sulle problematiche emerse e valutare possibili soluzioni.

Per questioni di metodo pare opportuno suddividere l'analisi in due parti che riprendono il titolo del contributo. Nella prima l'attenzione sarà rivolta all'uso degli algoritmi all'interno delle amministrazioni pubbliche. Si tratteranno, dunque, alcuni impieghi degli algoritmi da parte delle pubbliche amministrazioni, le problematiche che questi hanno fatto emergere e le soluzioni che il giudice amministrativo ha offerto. Quest'ultimo passaggio consentirà di vagliare la compatibilità dell'uso degli algoritmi nell'azione amministrativa e delle norme che attualmente li disciplinano con i due modelli di razionalità sopra richiamati. Per non incorrere in uno sterile e infondato binarismo tra accettazione e rifiuto della digitalizzazione dei procedimenti amministrativi si rivelerà opportuno inquadrare l'impiego delle tecnologie in un'ottica più ampia, quella, appunto, "dell'amministrazione pubblica degli algoritmi". Si argomenterà pertanto l'utilità di interpretare alcuni istituti del Codice dell'amministrazione digitale (CAD), come il riuso del software, quali strumenti di coordinamento informatico in grado di contribuire maggiormente all'ammodernamento delle amministrazioni contemperando le esigenze di differenziazione, da una parte, e preservando la riuscita della transizione digitale dall'altra. È in questa direzione che si proverà ad offrire nuovi spunti per valorizzare la normativa sul riuso del software.

2. L'impiego di ICTs nella pubblica amministrazione: i problemi e le tutele procedimentali

L'impiego di algoritmi all'interno della pubblica amministrazione appartiene ormai alla realtà.

Nella prassi amministrativa, infatti, si ha contezza del ricorso ad almeno due distinte tipologie di algoritmi. La prima è quella degli algoritmi condizionali, o deterministici. Questo primo gruppo di algoritmi consente di applicare regole predeterminate all'avverarsi di determinate condizioni. In sostanza è possibile trasporre in istruzioni informatiche, contenute nel codice sorgente, pienamente intellegibile da parte di un soggetto con adeguate competenze, le norme giuridiche che disciplinano una determinata attività amministrativa[10]. È il caso tipico dell'attività amministrativa vincolata, in cui l'assetto degli interessi è interamente predisposto dalla norma di legge, nell'ambito della quale il Consiglio di stato ha ritenuto adeguato l'impiego di elaboratori elettronici una «doverosa declinazione dell'art. 97 Cost.»[11]. L'impiego di questo tipo di algoritmi può certamente contribuire in maniera sensibile all'efficienza e all'efficacia dell'azione amministrativa. Esso consente, ad esempio, di accelerare lo svolgimento del procedimento con evidenti positive conseguenze sul rispetto dei termini di conclusione e, più in generale, agevola la gestione di grandi quantità di informazioni, altrimenti rimessa alle capacità di singoli e pochi funzionari, con un auspicato miglioramento del servizio reso[12].

Il secondo gruppo, invece, è quello degli algoritmi predittivi. Questi, impiegati nelle tecnologie di *machine learning*, sono composti da due elementi fondamentali: il *codice sorgente* e il *modello matematico*. In sostanza il sistema di *machine learning* genera dei parametri, sulla base di un patrimonio informativo, costituito da set di dati (input), che gli è stato fornito in fase di addestramento (cd. training). Lo stesso algoritmo è poi in grado di esaminare il grado di corrispondenza tra il risultato fornito e il modello matematico originario, consentendo così di determinare il grado di attendibilità della decisione assunta[13]. In tutti questi casi la decisione viene assunta mediante un raffronto tra la fattispecie concreta, la decisione assunta, e il modello matematico incorporato nel sistema.

Sebbene il processo di digitalizzazione della pubblica amministrazione sia ancora in corso e non completato, l'impiego di algoritmi, di entrambi i tipi, da parte delle pubbliche amministrazioni è, come si è detto, ormai un dato storico[14] e genera problemi diversi a seconda dell'amministrazione coinvolta, e quindi dell'interesse pubblico che si intende perseguire mediante il loro impiego.

L'impiego di siffatte tecnologie non assicura, come presumibile, la legittimità del provvedimento che conclude il relativo procedimento. È ormai pacifico, infatti, che eventuali errori nella programmazione si riverberano, inevitabilmente, nell'atto conclusivo. Ci si è chiesti, in particolare, se esistano tutele adeguate nei confronti dei provvedimenti amministrativi adottati tramite il ricorso ad algoritmi[15].

La questione dipende in parte dall'attuale livello di sviluppo della tecnologia. Come si è accennato all'inizio, infatti, gli algoritmi deterministici non destano particolari problemi dal punto di vista tecnico-giuridico. La loro struttura lineare e, soprattutto, la logica causale che li caratterizza, consentono al programmatore di ricondurre il risultato (output) dell'algoritmo alle informazioni fornite e alla sequenza dei comandi fissati nel codice sorgente. Conseguentemente l'amministrazione che dovesse ricorrere all'algoritmo avrebbe sempre gli strumenti per fornire all'interessato le informazioni sul trattamento dei dati e sulle ragioni della decisione che lo riguardano. Diverso discorso, invece, deve farsi con i sistemi di *machine learning*, i quali seguono logiche inferenziali e presentano quell'opacità che, secondo taluni, caratterizza la cosiddetta *black box society*[16]. Nei considerando del Regolamento generale sulla protezione dei dati (GDPR)[17] sembra ritrovarsi questa differenza ma ciò di cui si discute in dottrina è se effettivamente il regolamento europeo, che costituisce l'architrave della regolazione delle decisioni automatizzate, fornisca una copertura normativa e riconosca adeguati diritti agli interessati.

Il "diritto alla spiegazione" (*right to explanation*), infatti, può declinarsi in diversi modi a seconda del suo oggetto o al momento in cui si richiede la conoscenza delle ragioni delle decisioni. Con riguardo al primo si può chiedere una spiegazione sul "funzionamento del sistema", con specifico interesse alla logica sottesa al sistema, al suo modo di trattare le informazioni fornite, alla sequenza dei comandi che lo regolano. Oppure, si può richiedere di conoscere le esatte ragioni e variabili che hanno influito nell'assunzione di una "specifica decisione"[18]. Con riguardo al momento, invece, il diritto alla spiegazione può essere esercitato prima che una decisione e/o una valutazione venga assunta oppure successivamente[19].

Una parte della dottrina, allora, partendo dalle attuali possibilità tecniche, ha adottato un approccio *massimalista* verso le disposizioni del GDPR e ha sostenuto che gli strumenti di garanzia attuali, procedimentali e giurisdizionali, attualmente esistenti sono in grado di rispondere alle sfide poste dal *machine learning*[20]. Nei confronti di una decisione amministrativa adottata tramite un sistema di *machine learning*, infatti, il privato deve essere innanzitutto informato del fatto che i suoi dati hanno ricevuto un trattamento automatizzato ai sensi degli artt. 13 e 14 GDPR. Tale obbligo si pone come un onere aggiuntivo di *disclosure* sulle modalità con le quali l'amministrazione ha svolto l'istruttoria. In secondo luogo, nella parte motiva, la decisione adottata potrà fare riferimento al codice sorgente e al modello matematico impiegati. Infine, connesso al punto precedente, l'interessato che, volendo tutelare la propria situazione giuridica, ritenesse insoddisfacente la motivazione resa potrebbe proporre istanza di accesso documentale al codice sorgente e al modello matematico, finanche al data set. Questi, ultimi, infatti, secondo questo primo approccio, dovranno considerarsi a tutti gli effetti quali atti e documenti amministrativi[21], strettamente connessi ed essenziali al contenuto del provvedimento. Proprio questa loro funzione essenziale nel procedimento renderebbe l'accesso defensionale differibile o negabile ma mai recessivo «dinanzi alla tutela della proprietà intellettuale, ancorché coperta da brevetto»[22]. D'altra parte, si ritiene che «la sconoscenza del codice sorgente impedisce la tracciabilità primigenia dell'algoritmo, il fondamento stesso del meccanismo computazionale» con la conclusione di «escludere quel dovere esplicativo che le stesse raccomandazioni europee richiamano»[23]. Sul versante più propriamente giurisdizionale, invece, il giudice, nel sindacare la legittimità del provvedimento, potrà fare riferimento al margine di errore per valutare prioritariamente la corrispondenza della decisione assunta rispetto ai risultati forniti dall'algoritmo. Successivamente, nel caso in cui ci fosse corrispondenza tra modello e output, si potrebbe procedere all'esame della corrispondenza del modello stesso al caso (con conseguente denunzia dell'eccesso di potere in caso di travisamento dei fatti). Anche nei casi in cui l'illegittimità dovesse riguardare un atto presupposto, con le dovute analogie del caso come sopra ricostruite, le tutele azionabili potrebbero essere le medesime di quelle canonicamente previste nell'ordinamento, cioè l'impugnazione dell'atto definitivo e dei suoi presupposti[24].

Altri[25], invece, seguendo un approccio *minimalista* e interpretando restrittivamente le norme del GDPR, hanno ritenuto che un siffatto *right to explanation* avrebbe, e dovrebbe avere, un'estensione più ridotta.

Si è visto in particolare un limite interno dello stesso diritto proprio nel dato letterale dell'art. 22 GDPR, secondo cui, una volta assunta la decisione «data subjects are granted additional safeguards to obtain human intervention, express views, or contest a decision (Article 22(3)), but not to obtain an explanation of the decision reached»[26]. Nemmeno gli artt. 13 e 14 fornirebbero un'adeguata base normativa per una spiegazione *ex post*, perché, al contrario, essi si limiterebbero

a garantire la *explanaibility* del programma, in altri termini la logica ad esso sottesa, come sopra accennato. Anche il diritto di accesso previsto dall'art. 15 non servirebbe allo scopo. La sua costruzione "future-oriented"[27] lascia presumere che «the right of access is not addressing how an individual decision was reached, but rather the duty of the data controller to provide information about the existence, aims and consequences of such processing. This equates to an explanation of system functionality»[28], tornando dunque a limitare il diritto alla spiegazione solo *ex ante*.

Un secondo argomento a sostegno della limitatezza di un siffatto diritto, ed è quello che più interessa ai fini del presente contributo, si fonda sul carattere asseritamente recessivo del diritto d'accesso rispetto ad altri interessi, *in primis* la tutela della proprietà intellettuale sul codice sorgente. Gli artt. 13-15 GDPR, come si è visto, consentirebbero solo di fondare una pretesa ad una motivazione esaustiva delle ragioni alla base della decisione e del meccanismo di funzionamento del programma. Ma se questa è l'estensione del diritto, essa (i) non sarebbe in grado di radicare l'obbligo di ostendere il codice sorgente, che potrebbe costituire un segreto commerciale[29]; (ii) non sarebbe sufficiente a superare il test di proporzionalità, inteso in senso lato come comprensivo anche del principio di necessità. Prima di accedere al codice sorgente, infatti, bisognerebbe verificare se «le esigenze difensive – da valutare in concreto e non in astratto – possano essere soddisfatte in altro modo, ossia con un apparato informativo di diversa natura (rispetto all'insieme delle istruzioni in linguaggio di programmazione, di cui consta il codice sorgente)» e «se il codice sorgente, che si intende "aprire" in favore dell'interessato, abbia effettivamente l'attitudine a soddisfare le esigenze di difesa che questi vuole far valere»[30].

La giurisprudenza amministrativa, dopo alcune iniziali diffidenze[31] circa la compatibilità dei procedimenti automatizzati con la l. 241/1990[32], li ha ammessi a condizioni che si rispettino taluni principi di *legalità algoritmica*[33].

Infatti, per garantire quel diritto a conoscere la logica sottostante la decisione amministrativa (art. 13 co. 2 lett. f) GDPR), il giudice amministrativo ha ritenuto che l'algoritmo debba essere *trasparente* nel senso di riconoscere all'interessato un diritto a disporre del codice sorgente in quanto parte essenziale dell'algoritmo, da intendersi quale documento amministrativo, perciò suscettibile di accesso documentale[34].

In secondo luogo, la giurisprudenza ha posto l'accento sull'onere motivazionale dell'ufficio procedente, il quale dovrà anche in questi casi dare conto delle ragioni di fatto e di diritto che lo hanno indotto ad adottare un determinato provvedimento. Non è dunque ammesso che il provvedimento finale si limiti a recepire il risultato fornito dall'algoritmo, escludendo così l'ipotesi di procedimenti completamente automatizzati[35], nel rispetto del principio di non esclusività algoritmica[36], sancito dall'art. 22 GDPR. Questo onere motivazionale, nonostante i rilievi *in bonam partem* sopra formulati sulla corrispondenza della decisione al modello matematico, si presenta particolarmente gravoso quando si ricorre ai sistemi di *machine learning*, che ricorrono a logiche inferenziali difficilmente ricostruibili dagli stessi programmatori[37].

Infine, deve essere rispettato il principio di non discriminazione algoritmica, a tutela dai cd. *bias* algoritmici[38], il che richiede la massima attenzione alla qualità dei dati impiegati nel procedimento e all'adeguatezza della programmazione *ab origine*.

3. Alcune criticità sistemiche dell'impiego di ICTs nella pubblica amministrazione

La risolutezza nel sancire l'accessibilità al codice sorgente e la lenta gradualità nell'accettazione delle procedure automatizzate[39] suggeriscono la complessità del tema e la difficoltà di sciogliere il nodo della cd. *opacità* dell'algoritmo nonché quello della tutela della proprietà intellettuale del codice sorgente. È proprio su questo punto che trasparenza e proprietà intellettuale si mostrano come antagonisti. In assenza di un completo quadro normativo il giudice amministrativo, infatti, ha offerto soluzioni per recuperare la legalità dell'azione amministrativa nella dinamica del rapporto amministrativo e disegnare un sistema di tutele procedimentali – *technological due process*[40] – muovendosi, però, sempre in una logica binaria (amministrazione/amministrato), sulla base di un'asserita assimilabilità tra algoritmo e apparato[41]. Il rischio di questo approccio è quello di convogliare la discussione nel dualismo tra ammissione o rifiuto dell'impiego degli algoritmi nei procedimenti amministrativi in quei casi in cui le attuali tecnologie non consentano un esaustivo controllo dell'operato degli algoritmi.

Può essere utile interrogarsi, allora, sulle possibili cause di questa contraddizione per ipotizzare alcune soluzioni.

In primo luogo, si può osservare come l'analisi sopra riportata sia evidentemente rivolta alla garanzia della sfera giuridica del singolo e sviluppata nell'ambito di una tutela "atomizzata ed interna"[42] e come, in ogni caso, si punti esclusivamente ad un controllo successivo alla programmazione dell'algoritmo. Questo elemento influisce anche in sede procedimentale, poiché gli istituti tradizionali di partecipazione troveranno forti resistenze derivanti non tanto dal compor-

tamento tenuto dall'amministrazione ma, come visto, dai limiti esterni dettati proprio dalla tecnologia che si intende implementare e dalle modalità con le quali è stata programmata.

In secondo luogo, non si deve dimenticare, infatti, l'impianto di fondo del GDPR, cioè del principale strumento regolatorio in materia di amministrazione digitale attualmente vigente, il quale è chiaro nel fissare i fuochi dell'ellisse normativa sulla "protezione delle persone fisiche" e sulla "libera circolazione dei dati"[43]. È lo stesso diritto alla riservatezza che trova nel GDPR un limite esterno nella "funzione sociale"[44] del dato personale che al giurista italiano rivela *ictu oculi* la piena sovrapposizione tra il dato personale e il contenuto patrimoniale della proprietà privata[45]. È proprio tale impostazione di fondo, unita all'ineffettività degli strumenti partecipativi, che fa risuonare il monito che tempo addietro Stefano Rodotà rivolgeva al legislatore, per invitarlo a ponderare «la doppia dimensione sociale della raccolta delle informazioni», in quanto, «da un canto, questa è effettuata da soggetti organizzati, pubblici o privati che siano; dall'altro, essa riguarda gruppi o categorie o collettività e non soltanto individui isolati» rilevando l'insufficienza dello "schema del consenso"[46], dal momento che «i termini del rapporto [...] sono sostanzialmente alterati: ad un rapporto interindividuale si è ormai sostituita, nella materia qui considerata una situazione più complessa, nella quale confluiscono interessi non riducibili a quelli della coppia "raccoglitore di informazioni/individuo investigato"».

La prospettiva procedimentale adottata, dunque, non darebbe adeguato spazio alla complessità derivante dalla sistemica presenza di un controinteressato[47], *id est* chi detiene la privativa sul codice sorgente.

Sinteticamente e in altri termini, le tutele pensate dal giudice amministrativo e alcuni principi stabiliti nel GDPR puntano a ristabilire una razionalità strumentale dell'azione amministrativa consentendo al privato di ricostruirne la ragionevolezza rispetto ai suoi fini ma solo parzialmente, invece, riescono a fornirne una sua razionalità comunicativa.

È opportuno interrogarsi dunque sull'opportunità di riscoprire percorsi normativi e/o di valorizzare disposizioni presenti in grado di sopperire a questo deficit.

4. Il riuso del software come strumento di governo delle ICTs nell'amministrazione pubblica

In questa direzione uno spunto è offerto proprio da alcuni sostenitori dell'approccio minimalista[48], i quali, contestando la sovrapponibilità tra algoritmo e organizzazione pubblica hanno sottolineato la centralità dell'art. 69 CAD. Il co. 2, infatti, dispone che «al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni» queste devono sempre essere titolari di «tutti i diritti sui programmi e i servizi delle tecnologie dell'informazione e della comunicazione, appositamente sviluppati per essa». Tuttavia, questa regola soffre l'eccezione che la titolarità può non essere trasferita quando ciò «risulti eccessivamente oneroso per comprovate ragioni di carattere tecnico-economico».

È da questa prospettiva che riusciamo a cogliere la fragilità del bilanciamento operato dal giudice amministrativo che, non a caso, è maturato affrontando proprio un caso di applicazione dell'art. 69 CAD[49] su cui, dunque, è necessario soffermarsi.

Lo sfondo teorico del riuso dei software[50] da parte delle amministrazioni pubbliche è costituito dall'e-government[51], concetto «fondato essenzialmente sulla condivisione e sulla codecisione delle politiche d'innovazione fra tutti gli enti di un medesimo territorio» che «presuppone una concertazione per l'individuazione degli indirizzi strategici e degli interventi operativi»[52]. All'interno di questa cornice si distinguono due concetti: riuso dei dati pubblici e riuso dei software[53]. Il secondo si pone come *species* del primo e ricomprende quelle informazioni relative a «componenti tecnologiche (software in senso stretto)» e alla «documentazione tecnica (analisi, modelli dati, modelli organizzativi, strumenti per la re-ingegnerizzazione dei processi, moduli formativi, ecc.)»[54]. Il tema del riuso, in uno con le vicende del CAD, ha oscillato tra la razionalizzazione economica – intesa quale sostegno alla riduzione della spesa pubblica – e quella amministrativa – intesa quale strumento di semplificazione amministrativa[55].

Si possono scandire, ai soli fini espositivi, tre fasi dello sviluppo del riuso del software nel nostro ordinamento amministrativo[56], caratterizzate dalle diverse composizioni delle diverse volontà riformatrici.

In un primo momento, coincidente proprio con la prima positivizzazione del riuso del software, le due spinte sono appunto compresenti ma sembra più chiaro l'indirizzo di stampo economicistico. Infatti, all'art. 2 co. 3 del d.lgs. 12 febbraio 1993, n. 39, che introdusse l'obbligo per le amministrazioni di conservare la titolarità degli applicativi impiegati nei procedimenti, e alla "legge di semplificazione 1999", che diede *facoltà* alle amministrazioni di mettere i propri applicativi a disposizione delle altre, quale strumento di semplificazione dei rapporti interorganici[57], fece seguito in maniera più netta e definita lo scopo di riduzione della spesa pubblica. Con la legge finanziaria 2003, in un

quadro complessivo di razionalizzazione della spesa pubblica, si ritenne utile «al fine di assicurare una migliore efficacia della spesa informatica e telematica sostenuta dalle pubbliche amministrazioni» eliminare duplicazioni e inefficienze «promuovendo le migliori pratiche e favorendo il riuso»[58]. La logica sottesa era quella di generare economie di scala e ridurre i costi marginali estendendo quanto più possibile l'impiego dei software già in circolazione. Sulla spinta della riduzione della spesa pubblica, dunque, si svilupparono anche i primi modelli di regolazione dello sviluppo tecnologico che avrebbe dovuto essere promosso tramite indirizzi governativi negli investimenti secondo una «coordinata e integrata strategia»[59]. È in questo frangente che venne adottata la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico che vedeva nel riutilizzo dei software un modello da implementare per garantire un'adeguata infrastruttura a quella "società della conoscenza", che venne delineandosi come modello euristico nei documenti europei proprio agli inizi degli anni 2000[60]. Nei considerando della direttiva, infatti, si legge che l'uniformità dell'infrastruttura tecnologica del settore pubblico era un tassello strategico per la circolazione di *contenuti digitali*, che oggi, consapevoli delle più recenti riforme, chiamiamo *mercato digitale*[61].

La seconda fase, invece, si apre con l'entrata in vigore del CAD[62] che consolida[63] tutta la normativa che si era sviluppata nella prima fase[64] e dedica il capo VI proprio al riuso con gli artt. 68 e 69 disegna un prototipo di regolazione dell'open source[65] nell'amministrazione italiana[66]. In sostanza il legislatore sbarra con diverse paratie il percorso d'accesso delle amministrazioni verso l'acquisizione di software proprietari. In questa seconda fase, infatti, compresa la necessità di un intervento coordinato a livello nazionale, alle amministrazioni vengono richiesti adempimenti preliminari prima di procedere con l'indizione di bandi di gara per l'acquisizione di software sul mercato privato. Si prevedono così concorsi di idee e si intraprendono percorsi di standardizzazione richiedendo la sottoposizione dei documenti di gara al parere tecnico del CNIPA (art. 67). Contemporaneamente il legislatore vincola la discrezionalità delle amministrazioni fissando un ordine di priorità nella scelta delle tipologie del software (art. 68), conferendo la priorità allo sviluppo *in house* e, successivamente, ma comunque prima dell'outsourcing, il ricorso a software già impiegati da altre amministrazioni. Una volta compiuta la scelta dell'esternalizzazione, invece, le amministrazioni devono optare per software open source, rispetto a quelli proprietari. Infine, ribadisce l'obbligo della condivisione gratuita con altre amministrazioni dei software ottenuti mediante le precedenti modalità.

In questa seconda fase emerge una forte spinta per un'innovazione e una semplificazione che passino da interventi strutturali nell'organizzazione amministrativa prima che dell'attività[67]. Proliferano dunque le linee guida per l'implementazione di standard, vengono ampliati i compiti di studio e monitoraggio del CNIPA e, in generale, si assiste a continui interventi riformatori[68] della normativa che hanno minato gli intenti codificatori del CAD L'equilibrio più delicato che il Codice tenta di conservare è quello tra l'armonizzazione del sistema informatico nazionale e l'autonomia organizzativa dei governi locali, in un riparto di competenze alquanto frastagliato non solo tra diversi livelli di governo ma innanzitutto su quello centrale[69].

La terza fase, infine, comincia a maturare con l'adozione della prima agenda digitale italiana, nell'ambito della "Strategia Europa 2020"[70], la cui realizzazione viene affidata alla neocostituita Agenzia per l'Italia Digitale - AgID[71]. Questo nuovo organismo, sottoposto alla vigilanza e all'indirizzo della Presidenza del Consiglio, svolge la funzione di coordinamento informatico previsto dall'art. 117 co. 2 lett. r) Cost. Ad essa vengono assegnati i compiti prima spettanti al CNIPA[72], in particolare quello della predisposizione delle linee guida[73] per fissare gli standard tecnici e, tra le principali funzioni di coordinamento, quella di favorire il riuso di software tramite la raccolta delle informazioni e la loro pubblicità, mediante appositi registri, prima, e portali *ad hoc*, poi. Occorre sottolineare come, in questa seconda fase, l'attenzione si sia spostata sull'ampliamento della gamma di servizi che le amministrazioni devono fornire online. Da qui l'attenzione alla "strategia delle anagrafi"[74]: l'art. 2 d.l. 18 ottobre 2012, n. 179, sostituendo l'art. 62 CAD, introduce l'Anagrafe nazionale della popolazione residente per la successiva implementazione del domicilio digitale PEC); l'indice nazionale degli indirizzi PEC delle imprese e dei professionisti (INI-PEC); l'art. 6, co. 1, lett. d-*bis*), istituisce l'indice degli indirizzi PEC della PA e dei gestori di pubblici servizi; e poi i fascicoli sanitari elettronici introdotti a livello regionale e la successiva istituzione dell'anagrafe nazionale degli assistiti (A.N.A., con il nuovo art. 62-*ter* del CAD, introdotto dal co. 231, l. 27 dicembre 2013, n. 147), il *Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese* - SPID[75]. La riforma operata dal d.lgs. 26 agosto 2016, n. 179, e del successivo correttivo del d.lgs. 14 dicembre 2017, n. 217, opera in questa direzione per consolidare la centralità strategica dell'AgID e la realizzazione delle strategie digitali che si sono susseguite nel tempo, imprimendo nuova accelerazione alla digitalizzazione dell'amministrazione pubblica[76]. In quest'ultimo periodo si assiste a un'integrazione più pronunciata tra le politiche inter-

ne di digitalizzazione e gli atti normativi e di indirizzo europei contenuti nelle varie Agende digitali europee[77] che si sono susseguite ma, ancor di più, con l'adozione del GDPR e il più recente *Digital Market Act*[78]. Nel nuovo contesto normativo venutosi a delineare negli ultimi anni, è sempre più sfumato il movimento descritto dalle norme sul riuso dei software perché è ormai indiscussa la centralità della circolazione dei dati, soprattutto di quelli del settore pubblico[79]. L'attenzione al tema non è comunque diminuita se si considera che nel 2019 sono entrate in vigore le Linee Guida AgID sull'acquisizione e riuso di software per le pubbliche amministrazioni[80] con le quali l'Agenzia ha declinato l'opzione preferenziale del legislatore per la licenza open source, uniformando la disciplina dell'acquisizione dei software e delle procedure comparative (punto 2) fornendo le definizioni e le modalità di riuso e delle licenze open source (punti 1 e 3).

Ciononostante, i riscontri pratici offrono un quadro meno confortante segnando una differenza tra il riuso "annunciato" e quello "praticato". Infatti, nel recente referto della Corte dei conti[81], il riuso dei software è considerato esclusivamente tra le pratiche di razionalizzazione della spesa pubblica, apparentemente irrelato dagli altri obiettivi strategici, e così denunciando la mancata comprensione da parte del giudice contabile della portata sistemica del suo impiego. Non solo, nel documento le Sezioni di controllo constatano che «non è stata data evidenza di risultati concreti in tema di razionalizzazione degli applicativi attraverso il c.d. "riuso"». Non molto diversi i rilievi raccolti nel referto sullo stato di attuazione del Piano triennale 2017-2020[82], dove la Sezione Autonomie registrava un dato forse più allarmante e cioè che «il riuso del software [...] è risultato un tema sconosciuto a molti enti»[83].

Si comprende, dunque, l'accento posto nel nuovo Piano triennale 2020/2022 sul «rispetto degli obblighi del CAD in materia di open source al fine di massimizzare il riuso del software» per evitare i casi di «applicativi utilizzati da una singola PA e non condivisi tra più soggetti»[84]. Vista la lenta diffusione del riuso del software, infatti, nell'ultimo Piano triennale l'Agenzia ha fissato per le amministrazioni pubbliche l'obbligo di dichiarare – a partire da ottobre 2020 – all'interno del portale di *Developers Italia*, quali software di titolarità di un'altra PA esse hanno acquisito in riuso e di adeguare, entro ottobre 2020, le proprie procedure di procurement alle linee guida di AgID sull'acquisizione del software. Accanto a questi obblighi dichiarativi e conformativi, l'Agenzia ha stabilito per il 2020 una "baseline" di almeno 70 amministrazioni, che avrebbero dovuto rilasciare software open source in *Developers Italia* – il nuovo portale di raccolta dei software open source sviluppati ai sensi del nuovo art. 69 co. 1 – e almeno 600 soggetti che avrebbero dovuto riusare software open source presenti in *Developers Italia*. A queste soglie erano previsti incrementi annuali per tutto il periodo di vigenza del Piano. Tuttavia, nell'aggiornamento al Piano (2021-2023) è stata ripianificata al 30 giugno 2022 la predisposizione del portale sul quale le amministrazioni avrebbero dovuto caricare i loro applicativi open source, con presumibile ritardo sulle rimanenti e connesse scadenze[85], sebbene sia stato aumentato notevolmente il numero atteso dei soggetti coinvolti nel riuso dei software in corso di Piano[86].

5. (segue) Le potenzialità residue del riuso del software

Dopo il tracciato normativo esposto e i tentativi dell'Agenzia di promuovere il riuso del software – nato come una pratica da incentivare e divenuto un obbligo giuridico di cui a fatica si riesce a garantire l'effettività – si può concludere che gli artt. 68 e 69 CAD possono certamente contribuire alla digitalizzazione dell'amministrazione, in particolar modo nel miglioramento dell'erogazione dei servizi, ma difficilmente possono costituire un elemento portante di tale processo. In quest'ultimo paragrafo, allora, si vuole effettuare un ultimo tentativo in tal senso per valutare l'effettività marginalità di dette norme nel processo di digitalizzazione.

All'inizio del paragrafo precedente, infatti, si è mostrato come le tutele procedimentali attualmente proposte dalla dottrina e dalla giurisprudenza siano sufficientemente in grado di ricondurre l'azione amministrativa a una razionalità strumentale ma presentino criticità rispetto a quella comunicativa. Si è ipotizzato allora che il riuso del software, di cui agli artt. 68 e 69 CAD, potesse essere d'aiuto in tal senso. Sulla scorta di ciò, dunque, si è analizzata l'evoluzione degli artt. 68 e 69 CAD all'interno della più ampia evoluzione del Codice stesso. Resta da chiedersi allora se i rilievi svolti ci consentano di promuovere il riuso del software come strumento idoneo ad attivare procedure che consentano lo «scambio ragionato degli argomenti tra amministrazioni e destinatari dell'azione amministrativa», in modi variabili rispetto all'assetto degli interessi in gioco, circa l'interpretazione dei fini e l'individuazione dei mezzi[87].

Ebbene, si è constatato che il riuso dei software rimane un obiettivo da realizzare e che presso gli enti locali esso rimane un argomento pressoché sconosciuto. La soluzione proposta dall'ultimo Piano triennale a questi due problemi è stata quella di irreggimentare le amministrazioni fissando *milestone* comuni

monitorate con indicatori statistici[88], che in materia di riuso di software sono stati individuati in quantitativi di amministrazioni che ricorrono al riuso e/o che sviluppano software open source distribuendone poi le informazioni. Dalla mancata attuazione della norma, però, non possiamo dedurre nulla circa le sue possibili ricostruzioni teoriche.

Per proseguire nel tentativo, le Linee Guida AgID sul riuso del software ci aiutano fornendoci una suddivisione in macrofasi del procedimento amministrativo che le amministrazioni devono svolgere per acquisire un software e che in maniera plastica ci presentano in ordine logico: (i) l'individuazione delle esigenze; (ii) l'analisi delle soluzioni adottate dalle altre amministrazioni; residualmente, (iii) l'analisi delle altre soluzioni[89].

L'analisi delle prime due fasi ci mostra come alle amministrazioni venga richiesta un'attenta istruttoria su due versanti. Il primo è di tipo introflesso perché per giungere alla definizione delle esigenze l'amministrazione deve innanzitutto scandagliare le proprie attribuzioni[90]. Questo primo momento è imprescindibile per individuare gli strumenti mancanti e delineare i limiti della propria competenza. Il secondo, invece, estroflesso, pone l'amministrazione procedente nella condizione di interloquire con altre amministrazioni, anche tramite un portale di aggregazione – vedi *Developers Italia* – e individuare quelle con le quali condivide le proprie esigenze. Queste due dinamiche trovano sul piano giuridiche varie espressioni. Diversi, infatti, sono i principi di diritto amministrativo che trovano espressione in questo modo di procedere. Innanzitutto, si possono rinvenire in esso i principi di sussidiarietà, adeguatezza e differenziazione. Le amministrazioni coinvolte in questo procedimento sono infatti quelle prossime alle collettività cui è rivolta la loro azione e, poiché titolari prime delle funzioni amministrative, saranno esse stesse, e non potranno esserlo altri, a poter individuare i bisogni specifici. Saranno sempre questi principi, poi, a guidarle nella ricerca di soluzioni ottimali inducendole a ricercarle presso enti e/o apparati titolari di medesime funzioni. In secondo luogo, costruendo proprio su questo secondo livello, è ipotizzabile la valorizzazione dell'azione regionale[91]. Il tema non è peregrino e ha trovato modo di farsi spazio anche nella giurisprudenza costituzionale. Nell'ambito della materia del coordinamento informatico (art. 117 co. 2 lett. r) Cost.), infatti, la Corte ha già chiarito che tale coordinamento tende ad «assicurare una comunanza di linguaggi, di procedure e di standard omogenei, in modo da permettere la comunicabilità tra i sistemi informatici della pubblica amministrazione», nonché a «garantire la omogeneità nella elaborazione e trasmissione dei dati»[92]. Salvo alcuni casi[93], la potestà legislativa e le attribuzioni amministrative[94] sull'organizzazione e sulla disciplina delle reti informatiche entro cui far confluire i dati conoscitivi che sono nella disponibilità delle istituzioni regionali e locali o di altri soggetti interessati spettano alle Regioni[95]. Non a caso sono state le Regioni a prevedere i primi progetti open source per favorire il riuso, il risparmio sulla spesa pubblica, anche e soprattutto un canale di pluralismo informatico[96].

Sul piano sostanziale a livello regionale potrebbero svilupparsi prassi di coordinamento amministrativo tra strutture equiordinate[97], partendo proprio dall'applicazione di quell'analisi comparativa prevista dagli artt. 68 e 69 CAD, quale luogo di scambio degli "argomenti" dell'azione delle amministrazioni procedenti, intendendo con ciò l'affinamento delle esigenze in dialogo con sviluppatori non necessariamente privati e lasciando all'AgID il ruolo di predisporre la sola cornice degli standard tecnici. Anche in questa materia, dunque, vi sono margini per approfondire la "funzione sociale"[98] delle procedure comparative e le competenze di quegli apparati sorti a livello regionale che, a differenza dell'all'AgID, in forza del principio di sussidiarietà verticale, sarebbero pienamente titolati a svolgere sul territorio regionale un ruolo di coordinamento più intenso di quello svolto dall'organo nazionale. In questo contesto, allora, l'attuazione del binomio normativo sul riuso del software deve essere valorizzato come innesco di dinamiche di coordinamento amministrativo, quale «principio politico di organizzazione della complessità sociale»[99]. Su questo versante si può ipotizzare per il riuso dei software un ruolo strategico nella realizzazione delle agende digitali.

Per muoversi in questa direzione, però, è necessario costruire il coordinamento amministrativo non sulla classica sovrapposizione tra procedimento e comportamento amministrativo ma sulla dinamica del dovere d'ufficio[100]. Si intende con ciò quella diversa prospettazione che, partendo dalle criticità del concetto di coordinamento amministrativo[101], emerse nella sua evoluzione, vede come suo primo momento non la convocazione di una conferenza di servizi o l'istituzione di un organo preposto al coordinamento in chiave sovraordinata, ma la «acquisizione dello scenario di contesto in cui si inserisce l'agire di ciascuna articolazione amministrativa»[102]. In questa prospettiva acquisisce nuova importanza il tema della competenza che non costituirà più il limite esterno dell'esercizio del potere d'ufficio ma, piuttosto, il contenuto del dovere d'ufficio[103]. Come è stato sottolineato ciò richiede un cambio di paradigma poiché si tratta «certamente di un comportamento che impatta fortemente sulla razionalità amministrativa e sulle modalità in cui la stessa è spesa dal funzionario pubblico preposto

all'ufficio», dal momento che «questi sarà infatti tenuto ad operare tenendo conto di tutte le variabili relazionali [...], garantendo un costante e completo flusso di informazioni tra articolazioni amministrative e dunque modellando il proprio agire su quello degli altri soggetti coinvolti nell'interazione»[104].

6. Considerazioni conclusive

Si è visto come le tutele procedimentali approntate da letteratura e giurisprudenza aiutino a restituire all'azione amministrativa la sua razionalità strumentale ma non facciano altrettanto con riferimento a quella comunicativa. Questo deficit si esprime come dato sistemico perché pone l'interessato nella strettoia del *consenso*, che non considera gli elementi di fatto in grado di incidere sulla libera scelta del singolo. D'altra parte, invece, si è sottolineato il carattere antagonista che può assumere il rapporto tra proprietà intellettuale e trasparenza della decisione amministrativa. Interpretare il dato positivo degli artt. 68 e 69 CAD nella chiave da ultimo proposta sembra fornire elementi utili ad affrontare tali problematiche. Il coordinamento amministrativo, infatti, inteso come regola della funzione non come procedimento[105], consente di portare il bilanciamento degli interessi ad un livello collettivo che arriva a coinvolgere lo stadio in cui sono individuate le stesse regole sottese al funzionamento dei vari programmi informatici. Ciò consente di collegare il singolo procedimento amministrativo alla matrice più grande del processo di digitalizzazione e degli indirizzi che gli si vuole conferire. Sul piano della proprietà intellettuale, invece, l'azione coordinata di più amministrazioni può avere ad oggetto l'avvalimento delle reciproche risorse e conoscenze, che difficilmente potranno essere recepite sul mercato, perché maturate in seno all'esperienza pubblica; questo potrebbe fornire un criterio aggiuntivo per valutare in concreto l'opportunità di ricorrere a un applicativo proprietario invece di optare per il riuso di un software già in uso presso altre amministrazioni. Infine, agendo sul momento di acquisizione del programma si interverrebbe a monte sui problemi di bilanciamento sorti a valle nel tentativo di riconoscere un pieno diritto alla *explainability*. Sono questi gli elementi che in definitiva possono aiutare a ricostruire una razionalità non solo strumentale ma anche comunicativa dell'azione amministrativa quando, nel governo della complessità sociale, ricorre alle ICTs.

Note

[1]Cfr. V. Mayer Schomberger, K. Cukier, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà* (trad. it. R. Merlini), Garzanti, 2013; con attenzione al tema della pubblica amministrazione davanti a questo fenomeno, v. H. Broomfield, L. Reutter, *In search of the citizen in the datafication of public administration*, in "Big Data & Society", 2022, n. 1, p. 1 ss.

[2]Su tale fenomeno si veda A. Stazi, F. Corrado, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in "Il Diritto dell'informazione e dell'informatica", 2019, n. 2, pp. 443-487, dove si legge che «attualmente, i dati così raccolti possono essere utilizzati in quattro forme diverse: dati prodotti a livello individuale usati in modo non anonimo, relativi a individui-utenti o macchine specifici e tipicamente volti a fornire servizi agli individui stessi; dati raccolti a livello individuale usati in modo anonimo, ad esempio preferenze usate per il filtraggio collaborativo nell'ambito dei sistemi di raccomandazione dei film; dati prodotti a livello aggregato, quali ad esempio informazioni su profitti e perdite; dati contestuali, come quelli per le mappe. Inoltre, i dati possono essere generati a frequenze differenti e l'accesso ad essi può riguardare dati storici o in tempo reale». Sulla patrimonializzazione del dato, soprattutto del dato personale, vedasi *Personal Data: The "New Oil" of the 21st Century*, panel discussion at World Economic Forum on Europe and Central Asia 2011 (June 9, 2011); D.D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, February 10, 2014, in "Maine Law Review", vol. 66, 2014, n. 2, pp. 374-395, tutti ripresi da I. Speziale, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in "Contratto e impresa", 2021, n. 2, pp. 602-629; F. Midiri, *Proteggere i dati personali con le tutele del consumatore*, in "Giornale di diritto amministrativo", 2021, n. 5, pp. 609-620.

[3]N. Lettieri, *Contro la previsione. Tre argomenti per una critica del calcolo predittivo e del suo uso in ambito giuridico*, in "Ars Interpretandi", 2021, n. 1, pp. 83-96.

[4]Sulla relazione tra strumenti predittivi e diritto, si veda in chiave critica G. Zaccaria, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, in "Ars Interpretandi", 2021, n. 1, pp. 29-52, dove si legge che «Non si tratta insomma di contrapporre frontalmente, secondo una logica competitiva, l'uomo alla macchina, ancor più in un contesto in cui la relazione uomo-computer è divenuta sempre più penetrante e immersiva: non dobbiamo lasciarci chiudere nella tenaglia rappresentata dall'alternativa tra una accettazione acritica delle tecnologie informatiche ed un catastrofismo irrazionale che rifiuta la tecnologia paventando la fine del diritto, ma di capire che a tali tecnologie si lega una trasformazione profonda dei modi di costituzione del senso stesso del diritto, una sua ridefinizione simbolica e un'incidenza sulla stessa educazione del giurista, per non dire dei rischi legati alla tutela dei diritti, di cui dobbiamo avere piena consapevolezza». In generale si deve considerare che «la norma non si limita a descrivere un fatto generale e futuro, ma collega al suo accadere un effetto giuridico [...] l'individuo è in grado di calcolare ciò che avverrà» e la stessa circolarità logica del "decidere, giudicare e applicare la legge" – propria della forma processuale – poggia essenzialmente sul concetto di fattispecie; la quale «contiene la figura anticipatoria di ciò che accadrà; e traendolo indietro nel tempo lo rende prevedibile e calcolabile». Cfr. N. Irti, *Un diritto incalcolabile*, Giappichelli, 2016. Della crisi di questo modello lo stesso autore offriva lucide dimostrazioni fin da N. Irti, *L'età della decodificazione*, Giuffrè, IV ed., 1999. In senso contrario, per una critica alle tesi di N. Irti sopra esposta, si veda G. Corso, *Tra legge e fattispecie: la prospettiva del diritto amministrativo*, in "Ars Interpretandi", 2019, n. 1, pp. 71-90, *passim*, dove espressamente si legge che «nel diritto pubblico, e in particolare nel diritto amministrativo, le cose stiano diversamente: e, come dirò alla fine, penso che anche nel diritto privato la fattispecie goda tuttora di buona salute. È in

salute anche per effetto delle norme costituzionali che, secondo altra prospettiva, ne avrebbero determinato la crisi», a p. 74 ss.

[5]Il tema è evidentemente troppo ampio perché possa essere trattato in questa sede. Maggiore precisione imporrebbe infatti di declinare la capacità ordinante del diritto nelle sue manifestazioni storiche dello Stato di diritto e dello Stato costituzionale. V. sul punto G. Zagrebelsky, *Il diritto mite. Legge diritti giustizia*, Einaudi, 1992, p. 39 ss.; G. Azzariti, *La Costituzione come norma e la crisi del costituzionalismo contemporaneo*, in "Rivista italiana per le scienze giuridiche", 2013, n. 4, pp. 177-194, dove si enuclea il *proprium moderno delle costituzioni* nella loro capacità ordinante. Sul punto vedasi anche M. Fioravanti, *Passato, presente e futuro dello Stato costituzionale moderno*, in "Nomos. Le attualità nel diritto", 2018, n. 2. Parla di un "ritorno al futuro del costituzionalismo" nella società globalizzata, G. Allegri, *Il ritorno al futuro del costituzionalismo: un progetto di ricerca su spazi politici, soggetti sociali, nuove istituzioni*, in "Giornale di storia costituzionale", 2016, n. 32, pp. 131-149.

[6]E. Chiti, *Diritto amministrativo europeo. Stabilizzazione dei comportamenti e costruzione dell'ordine sociale*, in "Diritto Pubblico", 2015, n. 3, p. 910. Le categorie della razionalità strumentale e comunicativa si ispirano chiaramente, seppure non richiamate dall'autore, alle teorie dell'agire comunicativo di Habermas quale strumento di gestione della complessità sociale. Tuttavia si rinvengono, per diversa via, anche illuminanti riflessioni sulla funzione di riduzione della complessità sociale anche nella teoria dei sistemi complessi di N. Luhmann, così come letto da D. Fiorentino, *Conflittualità sociale e funzione immunizzante del diritto: qualche nota per una lettura sistemica della repressione penale politica nelle società complesse*, in A. Senaldi, X. Chiaramonte (a cura di), "Violenza politica. Una ridefinizione del concetto oltre la depoliticizzazione", Ledizioni, 2018, pp. 133-151, il quale osserva come «per Luhmann il diritto non solo rende i conflitti possibili, ma addirittura li produce, proteggendo il sistema non contro il "no", ma grazie all'ausilio della negazione, strumento privilegiato per preservare la società dall'annientamento o dall'implosione», a p. 135. Il diritto, dunque, non porterebbe alla produzione di ordine ma, al contrario, rinnoverebbe continuamente le condizioni di potenziali conflitti. Nell'ambito più strettamente giuridico il tema della razionalità strumentale è fortemente connesso a quello del principio di legalità per il quale si rimanda a M. Renna, F. Saitta (a cura di), *Studi sui principi di diritto amministrativo*, Giuffrè, 2012; in particolare M. Mazzamuto, *I principi costitutivi del diritto amministrativo come autonoma branca del diritto*, *ivi*, pp. 1-40; A. Bartolini, A. Pioggia, *La legalità dei principi di diritto amministrativo e il principio di legalità*, *ivi*, pp. 79-90; AA.VV., *Il principio di legalità nel diritto amministrativo che cambia*, Atti del LII Convegno di Studi sull'Amministrazione pubblica, Giuffrè, 2008; M. Immordino, A. Police (a cura di), *Principio di legalità e amministrazione di risultati*, Atti del convegno, Palermo 27-28 febbraio, 2003, Giappichelli, 2004. Inoltre, F. Merusi, *La legalità amministrativa. Altri sentieri interrotti*, il Mulino, 2012.

[7]Sul finalismo come caratteristica dell'azione amministrativa si rimanda per tutti a S. Cassese, *Le basi del diritto amministrativo*, Garzanti, 2000, p. 125.

[8]E. Chiti, *Diritto amministrativo europeo*, cit., p. 911.

[9]*Ibidem*.

[10]Sul punto si rinvia al contributo di G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in "Il Diritto dell'informazione e dell'informatica", 2021, n. 3, pp. 431-461, a p. 434, dove si svolge opportunamente anche la distinzione terminologica – che pare essenziale in questa fase degli studi sull'amministrazione digitale per chiarire la materia di cui si discute – tra algoritmi "condizionali" e "deterministici". Infatti, se i primi si basano su "conditional statements", quasi in termini di operatori booleani, i secondi, nella letteratura specialistica comprendono quegli algoritmi che, per determinati input, producono sempre il medesimo output (v. E. Peres, *Che cosa sono gli algoritmi*, Salani, 2020), sicché tra i modelli deterministici la letteratura informatica ricomprende a ben vedere anche molteplici tecniche di *machine learning* e *deep learning* in quanto — dato un certo modello — gli output del sistema sono anche in tali casi determinati univocamente dagli input, v. ad esempio J.Z. Liu, Z. Lin, S. Padhy et al., *Simple and Principled Uncertainty Estimation with Deterministic Deep Learning via Distance Awareness*, in "arXiv.org", 2020.

[11]Cons. St., Sez. VI, sent. n. 2270/2019 con nota di V. Canalini, *L'algoritmo come "atto amministrativo informatico" e il sindacato del giudice*, in "Giornale di diritto amministrativo", 2019, n. 6, pp. 781-787.

[12]Cfr. Cons. St., Sez. VI, sent. n. 2270/2019, cit.

[13]J.Z. Liu, Z. Lin, S. Padhy et al., *Simple and Principled*, cit., p. 437 ss.

[14]Tre esempi ci aiutano a capire e collocare all'interno dell'attività amministrativa questo gruppo di algoritmi. Il primo esempio è costituito dalle attività di controllo svolte dall'INPS In un'audizione del 2018 davanti alla Commissione Lavoro e Previdenza Sociale, il Garante della Privacy ha relazionato sull'impiego da parte dell'INPS del sistema SAVIO, che consentiva all'ente previdenziale di programmare l'attività ispettiva di visite fiscali per individuare quei casi in cui la condizione di malattia dichiarata non corrispondeva a quella reale. Il sistema richiedeva un trattamento automatizzato dei dati personali dei soggetti sottoposti a controllo e non era stato precedentemente notificato al Garante. Il secondo, invece, lo si ricava da un comunicato stampa del 4 marzo 2021 con il quale l'Agenzia delle Entrate informa che «si provvederà ad introdurre, a sperimentare e ad utilizzare tecniche innovative di network analysis, di machine learning e di data visualization, al fine di realizzare un nuovo sistema di supporto ai processi di individuazione dei soggetti ad alto rischio di frodi fiscali» ed è relativo al via libera dell'Unione europea al finanziamento del progetto "A data driven approach to tax evasion risk analysis in Italy". L'algoritmo dovrebbe essere operativo da luglio 2022. Tramite questo sistema (si tratta in particolare di un'architettura integrata che mira ad analizzare i dati posseduti dall'Agenzia attraverso diverse e differenti tecniche di inferenza, ciascuna delle quali costituita sull'impiego di molteplici algoritmi) l'Agenzia dovrebbe essere in grado di individuare con maggiore facilità, migliorando così l'attività ispettiva, i soggetti passibili di accertamento fiscale. Infine, in un comunicato stampa dell'8 giugno 2022, il Garante informa di aver attivato un'istruttoria su una pratica di *social scoring* nel Comune di Fidenza. La comunicazione si riferisce anche ad altre due istruttorie su analoghe pratiche di *social scoring* attuate nel Comune di Bologna. In particolare, una riguarda «il "Progetto Pollicino", un'indagine statistica a carattere sperimentale – promossa dalla Fondazione per lo sviluppo sostenibile, dal Ministero della transizione ecologica e dal Ministero delle infrastrutture e della mobilità sostenibili – attraverso la quale il cittadino viene invitato a condividere i propri dati (apparentemente "in forma anonima"), per consentire un'analisi della mobilità»; la seconda, invece, è relativa all'«iniziativa "smart citizen wallet" del Comune di Bologna, nell'ambito della quale è previsto che i cittadini possano aderire su base volontaria ad un sistema che consente di accumulare "crediti" all'interno del proprio "wallet" (portafoglio), da spendere accedendo ad una serie di premi/incentivi messi a disposizione dal Comune e da partner accreditati». Il Garante ha manifestato perplessità nei confronti del sistema della "Carta dell'assegnatario" che prevede l'attribuzione di un punteggio e/o di premi in base ai comportamenti assunti dai soggetti che volontariamente si prestano a

fornire i propri dati per la futura elaborazione da parte dell'ente locale, che potrebbe giungere sulla base di tali elaborazioni «alla risoluzione e/o la decadenza del contratto di locazione».

[15]Cfr. D.-U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2020, n. 3-4, pp. 501-516, a p. 515, ripresa da F. Nassuato, *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*, in "CERIDAP.eu", 24 novembre 2021, che vede nel procedimento il "luogo di elezione" per l'analisi dell'impatto della digitalizzazione sul diritto amministrativo, con particolare riferimento all'individuazione delle «regole che devono essere necessariamente rispettate, affinché il sistema di garanzie su cui si fonda lo "Stato di diritto" (e, nel nostro caso, "di diritto amministrativo") resti intatto».

[16]Cfr. F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015; S. Del Gatto, *Potere algoritmico, Digital Welfare State e garanzie per gli amministrati. I nodi ancora da sciogliere*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2020, n. 6, pp. 829-855.

[17]Regolamento UE 679/2016.

[18]Cfr. considerando 71 GDPR.

[19]Per questa schematizzazione si rinvia *amplius* a S. Wachter, B. Mittelstadt, L. Floridi, *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, p. 81 ss.

[20]Cfr. G. Carullo, *Decisione amministrativa*, cit., *passim*, in particolare p. 454.

[21]Sull'atto amministrativo informatico si rinvia a A. Masucci, *L'atto amministrativo informatico: primi lineamenti di una ricostruzione*, Jovene, 1993; Id., *Atto amministrativo informatico*, in "Enciclopedia del diritto", Aggiornamento vol. I, Giuffrè, 1999; Id., *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in "Rivista di diritto civile", 2004, n. 5, pp. 749-786; S. Puddu, *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, Jovene, 2006, p. 122 ss. Di particolare profitto, in ogni caso sul tema anche, e per tutti, A. Masucci, *Il documento amministrativo informatico*, Maggioli, 2000, p. 17 ss.; sulla differenza tra atto e documento informatico, Id., *Il documento amministrativo informatico*, in G. Arena, M. Bombardelli, M.P. Guerra, A. Masucci, "La documentazione amministrativa", Maggioli, 2001, p. 174 ss. Da ultimo, Id., *L'automatizzazione delle decisioni amministrative algoritmiche fra "big data" e "machine learning". Verso l'"algocratic governance"?*, in "Diritto e processo amministrativo", 2022, n. 2, pp. 265-313. Vedi in generale sulla giurisprudenza amministrativa intervenuta sul ricorso agli algoritmi da parte dell'amministrazione, R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in "Diritto amministrativo", 2019, n. 4, pp. 773-792.

[22]N. Paolantonio, *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi. (Sul controllo giudiziario delle "decisioni algoritmiche")*, in "Diritto amministrativo", 2021, n. 4, pp. 813-838; in termini v. anche V. Canalini, *L'algoritmo come "atto amministrativo informatico"*, cit.

[23]*Ibidem*.

[24]Cfr. G. Carullo, *Decisione amministrativa*, cit.

[25]F. Bravo, *Trasparenza del codice sorgente e decisioni automatizzate*, in "Il Diritto dell'informazione e dell'informatica", 2020, n. 4-5, pp. 693-724; Id., *Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional Balancing of Interests?* in "European Review of Digital Administration & Law", 2020, n. 1-2, p. 157 ss.; S. Wachter, B. Mittelstadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist*, cit.

[26]*Ivi*, p. 8.

[27]La norma fa riferimento alle "envisaged consequences".

[28]*Ivi*, p. 18.

[29]*Ivi*, p. 29.

[30]F. Bravo, *Trasparenza del codice sorgente*, cit., p. 700 ss.; Id., *Software di Intelligenza Artificiale e istituzione del registro per il deposito del codice sorgente*, in "Contratto e impresa", 2020, n. 4, pp. 1412-1429, a p. 1417, dove si specifica che «in una tecnica di bilanciamento proporzionale degli interessi volta a far salva la segretezza del codice sorgente s'è scelto di applicare il principio di trasparenza mediante un adeguato flusso informativo, funzionale agli obiettivi di tutela dell'interessato. Siffatta tutela però non deve riguardare l'accesso al codice, ma la correttezza e l'esaustività delle informazioni (altre rispetto alle istruzioni presenti nel codice sorgente) da fornire all'interessato, al fine di garantire quei diritti che l'ordinamento gli riconosce, primo tra tutti quello alla dignità personale e agli altri diritti fondamentali incisi dalle decisioni automatizzate e dai software di intelligenza artificiale, incluso quello di difesa giudiziale avverso le decisioni medesime». In termini anche E. Prosperetti, *Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del Tar Lazio*, in "Il Diritto dell'informazione e dell'informatica", 2019, n. 4-5, pp. 979-1010, nel quale si critica l'indirizzo giurisprudenziale maggioritario cui si era adeguato TAR Lazio n. 3769/2017.

[31]Per tutte si veda Cons. St., sez. VI, n. 2270/2019, cit., ma anche la successiva n. 8472/2019, con nota di A. Mascolo, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in "Giornale di diritto amministrativo", 2020, n. 3, pp. 366-375 e le successive sentt. nn. 8473, 8474 del 2019; cfr. F. Costantino, *Algoritmi, intelligenza artificiale e giudice amministrativo*, in "Giurisprudenza italiana", 2022, n. 6, pp. 1527-1536.

[32]T.A.R. Lazio, sez. III bis, 10-13 settembre 2019, n. 10964, dove si legge che «un algoritmo, quantunque, preimpostato in guisa da tener conto di posizioni personali, di titoli e punteggi, giammai può assicurare la salvaguardia delle guarentigie procedimentali che gli artt. 2, 6, 7, 8, 9, 10 della legge 7.8.1990 n. 241 hanno apprestato» riportata anche in E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2, pp. 273-304, a p. 276, il quale individua tre fasi della giurisprudenza amministrativa sulla cd. legalità algoritmica.

[33]E. Carloni, *I principi della legalità algoritmica*, cit.; cfr. Cons. Stato, sez. VI, sentt. 881/2020 e 1206/2021; si rinvia anche a S. Civitarese Matteucci, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in "Diritto Pubblico", 2019, n. 1, pp. 5-41.

[34]Questo indirizzo giurisprudenziale aderisce dunque alle tesi che interpretano integralmente l'algoritmo come atto amministrativo informatico.

[35]Cfr. D. Marongiu, *Algoritmo e procedimento amministrativo: una ricostruzione*, in "Giurisprudenza italiana", 2022, n. 6, pp. 1515-1523.

[36]Cfr. TAR Campania, Sez. III, n. 7003/2022, dove si afferma che «tra le indicate garanzie assume primaria importanza il rispetto del principio di trasparenza, che, com'è noto, trova un immediato corollario nell'obbligo di motivazione degli atti amministrativi ex art. 3 l. 241/90 e che non può essere soppresso né ridotto sol per la presenza di un algoritmo all'interno dell'iter procedimentale».

[37]Cfr. Cons. St., n. 7891/2021, dove al punto 9.1 si chiarisce che nei meccanismi di *machine learning* il sistema «non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra

dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

[38]Si veda G. Giorgini Pignatiello, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle* Digital authorities*?*, in "federalismi.it", 2021, n. 16, pp. 164-185, a p. 169; G. Resta, *Algoritmi, diritto, democrazia*, in "Giustiziacivile.com", 2019, n. 4, p. 4.

[39]Cfr. S. Sassi, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in "Analisi giuridica dell'economia", 2019, n. 1, pp. 109-128, a p. 119, la quale osserva che «l'azione amministrativa robotizzata, quale espressione del potere pubblico di autorganizzazione, non ha destato profili di illegittimità. il giudice amministrativo ha giudicato inammissibile la surrogazione dell'attività amministrativa da parte di una macchina algoritmica nel momento propriamente decisionale».

[40]Cfr. E. Carloni, *I principi della legalità algoritmica*, cit., *amplius* D.K. Citron, *Technological due process*, in "Washington Law Review", 2007, n. 85, p. 1304 ss., la quale individua i seguenti principi: *securing meaningful notice, protections for hearings; replacing rulemaking procedures*; D.K. Citron, F. Pasquale, *The Scored Society: Due Process for Automated Predictions*, in "Washington Law Review", 2014, n. 89.

[41]Cfr. TAR Lazio, Sez. III-*bis*, sent. n. 7526/2020, dove si legge che «in ragione della stretta correlazione tra requisito oggettivo (qualificazione dell'oggetto dell'accesso in termini di documento amministrativo) e requisito soggettivo (interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente collegata al documento) dell'istanza di accesso agli atti formulata ai sensi della legge n. 241/90, fondamentale, anche da un punto di vista logico, appare la riconducibilità del "codice sorgente" del programma informatico utilizzato per la gestione delle prove scritte del concorso, nell'ambito della definizione di "documento amministrativo" di cui alla lett. d), comma 1, art. 22 della legge 241 del 1990».

[42]S. Rodotà, *Elaboratori elettronici e controllo sociale*, il Mulino, 1973, p. 53, per il quale il «carattere atomizzato della tutela consiste nel fatto che: gli strumenti di controllo possono essere e utilizzati solo per iniziativa individuale; l'azione ha come unico sbocco la via giudiziaria; le conseguenze di essa riguardano unicamente i rapporti tra colui il quale ha agito in giudizio ed il soggetto che ha raccolto e diffuso le informazioni. Inoltre, il singolo non sempre è in grado di cogliere il senso che la raccolta di determinate informazioni può assumere in organizzazioni estremamente complesse o dotate di mezzi sofisticati per il trattamento delle notizie sì che gli sfugge lo stesso grado di pericolosità dell'impiego di quelle informazioni da parte di organizzazioni del tipo indicato».

[43]Si veda sul punto anche Commissione europea, *Una strategia europea per i dati*, COM(2020) 66 final, del 19 febbraio 2020, che promuove la creazione di quello «spazio europeo dei dati» e le considerazioni di L. Ammannati, *I signori dell'algoritmo*, in "Diritto Pubblico", 2021, n. 2, pp. 381-414, a p. 383, nota 5, nella quale si si chiarisce che il mercato dei dati «in quanto spazio comune dovrebbe rappresentare un superiore punto di riferimento. A questo si dovrebbe accompagnare la realizzazione di spazi comuni europei di dati in settori economici strategici e ambiti di interesse pubblico rendendo disponibili grandi pool di dati. Nella visione attuale della Commissione si prospetta una "legge sui dati" destinata a promuovere la condivisione dei dati principalmente tra imprese (B2B) ma anche tra imprese e pubblica amministrazione e viceversa».

[44]Considerando n. 4 GDPR.

[45]Cfr. I. Speziale, *L'ingresso dei dati personali*, cit., la quale sottolinea a ragione i «rischi connessi a una sostanziale mercificazione della persona»; cfr. anche A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in "Contratto e impresa", 2017, n. 2, pp. 586-612.

[46]Su tale conclusione converge anche la dottrina più recente. In particolare, con riferimento alla 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, G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, in "Giurisprudenza Italiana", 2019, n. 7, p. 1677, sostiene che «la logica del Regolamento è sempre basata sul dato personale rispetto al cui trattamento una determinazione viene espressa dal singolo individuo: l'interessato controlla e, in taluni casi, gestisce il suo dato seguendone la circolazione. Altre basi giuridiche concorrono a legittimare il trattamento dei dati personali, ma il modello culturale, prima ancora che giuridico, sul quale si base il Regolamento è quello dell'autodeterminazione. Tale logica, benché mitigata dall'accountability, non può essere applicata a grandi masse di dati, ai big data. Non è possibile pensare ad una gestione di tipo individuale dei dati, tanto meno se basata sul consenso. Il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace. Ciò tanto più se ci si confronta con applicazioni di intelligenza artificiale basate sui big data, nelle quali la determinabilità a priori dei processi di elaborazione non è scontata e nelle quali la finalità del trattamento sovente non è chiara». Sulla centralità del consenso vedasi anche T.M. Ubertazzi, *Ripensando alla revoca del consenso nella prospettiva funzionale della privacy*, in "Contratto e impresa", 2022, n. 1, pp. 27-51; A. Astone, *Autodeterminazione nei dati e sistemi A.I.*, in "Contratto e impresa", 2022, n. 2, pp. 429-448.

[47]Sulla problematica dei diritti dei terzi nel procedimento amministrativo vedasi in maniera più approfondita L. De Lucia, *Provvedimento amministrativo e diritti dei terzi*, Giappichelli, 2005.

[48]F. Bravo, *Trasparenza del codice sorgente*, cit., p. 693 ss.

[49]Cfr. TAR Lazio, Sez. III-*bis*, n. 7526/2020.

[50]Per un commento sul riuso del software nei primi anni successivi al CAD si veda V. Ambriola, G.A. Cignoni, C. Flick, *Riuso del software nella Pubblica Amministrazione*, in "Diritto dell'Internet", 2005, n. 1, pp. 85-91, in cui il riuso «tema emergente nel contesto dell'e-government, è inteso come adozione su scala più larga di soluzioni software locali, sviluppate autonomamente da singoli enti o da piccoli gruppi di enti, selezionate in base alle migliori caratteristiche rispetto ad altri prodotti software».

[51]In generale sul tema si veda F. Merloni (a cura di), *Introduzione all'eGovernment*, Giappichelli, 2005; G. Vesperini (a cura di), *L'e-Government*, Giuffrè, 2004; F. Musella, *Quale politica per il governo elettronico in Italia: costitutiva, distributiva o simbolica?*, in "Rivista internazionale di scienze sociali", 2007, n. 1, pp. 31-52; C. Batini, *Un'introduzione ai servizi di «eGovernment»*, in "Amministrare", 2013, n. 1, pp. 37-58; E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in "Diritto Pubblico", 2019, n. 2, pp. 363-391; A. Masucci, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in "Diritto Pubblico", 2020, n. 3, pp. 943-979.

[52]Sul riuso del software nell'amministrazione pubblica si veda F. Bargellini, M. Cherubini, *Il riuso nella società dell'informazione: un'opportunità per l'innovazione di sistema nella P.A.*, in "Informatica e diritto", 2006, n. 2, pp. 129-158.

[53]*Ivi*, p. 132.

[54]*Ibidem*.

[55]Di questi due versanti parla anche S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in "Giornale di storia costituzionale", 2016, n. 31, pp. 185-199, a p. 187.

[56]Cfr. F. Bargellini, M. Cherubini, *Il riuso*, cit.

[57]Art. 25 co. 1 l. 24 novembre 2000, n. 340 "Le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 3 febbraio 1993, n. 29, che siano titolari di programmi applicativi realizzati su specifiche indicazioni del committente pubblico, hanno facoltà di darli in uso gratuito ad altre amministrazioni pubbliche, che li adattano alle proprie esigenze".

[58]Cfr. art. 26 l. 27 dicembre 2002 (Legge finanziaria 2003).

[59]*Ibidem*.

[60]Cfr. le Conclusioni del Consiglio europeo di Lisbona del 23 e 24 marzo 2000.

[61]È interessante notare come già all'epoca il riutilizzo incontrava il limite dei diritti di proprietà intellettuale sul codice sorgente (cfr. cons. 22 direttiva 2003/98/CE).

[62]D.lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, integrato e modificato dal d.lgs. 4 aprile 2006, n. 159, Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale. Per primi commenti si veda E. Carloni (a cura di), *Codice dell'amministrazione digitale. Commento al D.Lgs. 7 marzo 2005, n. 82*, Maggioli, 2005; G. Frosio, *Guida al Codice della Pubblica Amministrazione Digitale. La digitalizzazione della P.A. alla luce del D.Lgs. 7 marzo 2005, n. 82*, Simone, 2005, anche riportati in G. Penzo Doria, *L'informaticrazia e il Codice dell'amministrazione digitale*, in "AIDAinformazioni", 2006, n. 3-4, p. 81; G. Cammarota, *Le modifiche al Codice dell'amministrazione digitale*, in "Giornale di diritto amministrativo", 2006, n. 9, pp. 943-948; M. Mancarella, *Profili negoziali e organizzativi dell'amministrazione digitale*, Tangram Edizioni Scientifiche, 2009, in particolare da p. 215 ss.

[63]Si è parlato di un irrigidimento dell'intera normativa in tema di informatica pubblica, per riferirsi, ad esempio, alla grande mole di articoli che da norme secondarie contenute ad esempio nel DPR. 445/2000 sono divenute primarie per effetto della loro trasposizione nel CAD, sul punto vedasi A. Natalini, *La semplificazione e la digitalizzazione*, in "Giornale di diritto amministrativo", 2005, n. 8, pp. 809-812, a p. 810.

[64]E. Massella, D. Teri, *Il Codice dell'amministrazione digitale: come evolve la normativa*, in "AIDAinformazioni", 2006, n. 3-4, p. 76, dove si parla di «costituzione del mondo digitale, che tiene conto di diritti e doveri e che contemporaneamente fornisce gli strumenti operativi giuridicamente validi con cui concretizzarli».

[65]Sull'impiego di programmi open source nell'amministrazione italiana si rinvia a S. Del Gatto, *I sistemi proprietari, l'"open source" e la pubblica amministrazione*, in "Giornale di diritto amministrativo", 2021, n. 5, pp. 571-577; nonché per le loro differenze a A. Palmieri, *Open source e contratti di assistenza*, in "AIDA", 2004, n. 1, pp. 281-302, e a V. Zeno Zencovich, P. Sammarco, *Sistema e archetipi delle licenze open source*, *ivi*, pp. 234-268, a p. 252 ss., *ivi* richiamati.

[66]Fin da subito il CAD è stato oggetto di numerose critiche per il suo carattere frastagliato e per l'imprecisione di alcune definizioni che lo porteranno a essere oggetto di innumerevoli riforme negli anni successivi. Il Codice che voleva coordinare la trasformazione digitale, infatti, fu pensato e redatto secondo un'impostazione *a silos* che vide protagonisti il Ministero per l'Innovazione e le Tecnologie e il CNIPA (Istituito dall'art. 176 del d.lgs. 30 giugno 2003 n. 196), sul punto vedi G. Penzo Doria, *L'informaticrazia*, cit. A ciò aggiungasi la contraddittorietà insita nella previsione della clausola di invarianza finanziaria con la quale si pretendeva di riformare l'intero apparato amministrativo senza nuovi investimenti.

[67]Una prova ne è il fatto che il Codice è stato curato dalle strutture del Dipartimento della Funzione pubblica (per gli istituti di semplificazione) e da quello dell'Innovazione tecnologiche, sebbene all'epoca ancora poco integrati. Sul punto vedasi A. Natalini, *La semplificazione e l'amministrazione digitale*, in "Giornale di diritto amministrativo", 2008, n. 1, pp. 105-111, a p. 105.

[68]Si veda in particolare l'intervento del d.lgs. 30 dicembre 2010, n. 235; per un commento vedi E. Carloni, *La riforma del Codice dell'amministrazione digitale*, in "Giornale di diritto amministrativo", 2011, n. 5, pp. 469-476.

[69]Non è mancato chi ha visto nel CAD uno strumento di sottrazione delle funzioni amministrative dai governi locali verso "il vertice, al centro", sull'errato assunto che "vertice e centro siano coincidenti"; v. sul punto L. Torchia, *Il riordino dell'amministrazione centrale: criteri, condizioni e strumenti*, in "Diritto Pubblico", 1999, n. 3, pp. 689-715, a p. 699; A. Natalini, *La semplificazione e la digitalizzazione*, in "Giornale di diritto amministrativo", 2005, n. 8, pp. 809-812, a p. 811; Id., *La semplificazione e l'amministrazione digitale*, in "Giornale di diritto amministrativo", 2008, n. 1, pp. 105-111, a p. 106. Pur registrando il centralismo legislativo, altri hanno sottolineato come più problematico il mancato rispetto del principio di adeguatezza delle strutture ministeriali all'epoca preposta all'attuazione del CAD, v. E. Carloni, *La riforma del Codice*, cit., p. 476.

[70]Comunicazione COM(2010) 2020, *Europa 2020: Una strategia per una crescita intelligente, sostenibile e inclusiva*.

[71]Artt. 19 ss., d.l. n. 83 del 2012; sul suo ruolo all'interno della governance amministrativa della digitalizzazione si F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in "Il Diritto dell'informazione e dell'informatica", 2015, n. 2, pp. 227-273.

[72]V. nota 66.

[73]Sulle linee guida nel sistema delle fonti si vedano: R. Bin, *Critica della teoria delle fonti*, FrancoAngeli, 2021; E. D'Orlando, F. Nassuato, *Linee guida e sistema delle fonti: un'ipotesi ricostruttiva*, in "Corti supreme e salute", 2021, n. 1, p. 55; G. Tropea, *Norme tecniche e "soft law"*, in "Nuove autonomie", 2022, n. 2, pp. 425-447.

[74]Cfr. S. Calzolaio, *Digital (and privacy) by default*, cit.

[75]*Ivi*, p. 191, il quale registra che «non vi è modo migliore di svelare la portata innovativa ed il rilievo giuridico istituzionale della digitalizzazione pubblica che semplicemente osservare come – nell'ordito del d.l. n. 179 del 2012 – essa operi ed incida silenziosamente sulle fondamenta stessa dello Stato moderno. Utilizzando il lessico tipico dell'era digitale potremmo dire che tale strategia fa leva su quanto di più immediatamente connesso possa esservi con la digitalizzazione e con internet: le basi di dati pubbliche (database). Secondo il lessico tradizionale, si può osservare che la strategia adottata si fonda sugli "archivi e registri pubblici"».

[76]Parla di nuova fase B. Carotti, *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in "Giornale di diritto amministrativo", 2017, n. 1, pp. 7-18; per un commento al correttivo si veda sempre B. Carotti, *Il correttivo al Codice dell'amministrazione digitale: una meta-riforma*, in "Giornale di diritto amministrativo", 2018, n. 2, pp. 131-141.

[77]Sulle quali vedasi in particolare COM(2021) 118, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, del 9 marzo 2021.

[78]Regolamento (UE) 2022/1925 del 14 settembre 2022 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).

[79]Il tema non è propriamente nuovo. Infatti, già il d.lgs. 24 gennaio 2006, n. 36 che recepiva la direttiva 2003/98/CE relativa al riutilizzo di documenti del settore pubblico aveva sottolineato l'importanza di regolare l'accesso al patrimonio informativo delle amministrazioni pubbliche che si caratterizzava per la mole e per la qualità. L'importanza di ciò derivava dal carattere essenziale di ingenti moli di dati per l'instaurazione di un mercato unico digitale e la necessità di impedire

effetti distorsivi della concorrenza causati proprio da condotte anticoncorrenziali da parte delle amministrazioni pubbliche nel momento di consentire l'accesso ai propri dati. Per un'attenta disamina del d.lgs. e per le criticità che solleva la logica proprietaria dei dati pubblici si rinvia a B. Ponti, *Il riutilizzo di documenti del settore pubblico*, in "Giornale di diritto amministrativo", 2006, n. 8, p. 817.

[80] Le *Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni*, in "Gazzetta Ufficiale", n. 119 del 23 maggio 2019, sostituiscono la precedente circolare 63/2013, intitolata *Linee guida per la valutazione comparativa prevista dall'art. 68 del C.A.D. e i relativi allegati*. Per un commento v. P. Falletta, *Le linee guida dell'agenzia per l'Italia digitale*, in "Giornale di diritto amministrativo", 2021, n. 2, pp. 163-171.

[81] Corte dei conti, referto 26 novembre 2019 e presentazione del referto.

[82] Disponibile sul sito della Corte dei conti.

[83] *Ivi*, p. 66.

[84] Cfr. AgID, Piano triennale per l'Informatica nella Pubblica Amministrazione 2020/2022, p. 10. Sempre *ivi* si veda tra gli obiettivi e i risultati attesi si ritrova «OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali», a cui è rivolta, tra le altre, l'azione «R.A.1.1a - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AgID sull'acquisizione e il riuso del software per la Pubblica Amministrazione».

[85] Vedi *Piano triennale 2021-2023*, p. 9.

[86] Ad oggi il target risulta parzialmente raggiunto.

[87] Cfr. E. Chiti, *Diritto amministrativo europeo*, cit., p. 911.

[88] Cfr. S. Del Gatto, *I sistemi proprietari*, cit.

[89] AgID, *Linee guida su acquisizione e riuso*, cit., p. 10.

[90] Sulla necessità che il legislatore guidi l'amministrazione in questa direzione si veda B. Marchetti, *The algorithmic administrative decision and the human in the loop*, in "BioLaw Journal", 2021, n. 2, «occorrerebbe procedere alla formulazione di principi e linee guida che orientino la p.a. non solo sul versante del rapporto con il cittadino ma sul versante interno, fornendo una cornice unitaria entro cui collocare le scelte sul ricorso all'IA, i vantaggi e gli svantaggi connessi ai diversi sistemi esperti, la tipologia di procedure sostituibili con procedure automatizzate», a p. 381.

[91] L. Reggi, C.A. Ricci, *Il ruolo delle società in house nel coordinamento delle politiche regionali per l'e-government*, in "Economia e Politica Industriale", 2014, n. 3, pp. 159-177.

[92] Corte cost. sent. n. 133/2008, ma anche la precedente sent. n. 17 del 2004.

[93] V. la conduzione coordinata ed integrata del sistema statistico ed informatico nel settore del lavoro (Corte cost. sent. n. 50/2005; istituzione di un sistema informatico nazionale di rilevamento ottico e di trasmissione telematica dei dati desumibili dalle ricette mediche e dalle confezioni dei farmaci (Corte cost. sent. n. 240/2007). Entrambe riprese da P. Costanzo, *Competenza legislativa regionale e programmi informatici open source*, in "Giurisprudenza costituzionale", 2010, n. 2, pp. 1437-1446.

[94] Sul rapporto tra le due si veda la storica sentenza Corte Cost. n. 303/2003 e i commenti di A. Morrone, *La Corte costituzionale riscrive il titolo V?*, in "forumcostituzionale.it", 2003; L. Torchia, *In principio sono le funzioni (amministrative): la legislazione seguirà*, in "astrid-online.it".

[95] Corte Cost. n. 122/2010, con nota di P. Costanzo, cit.

[96] Si vedano la L.R. Piemonte n. 9 del 2009; cui si fa riferimento nel testo; ma anche L.R. 25 luglio 2006, n. 11 della Regione Umbria o legge della Regione Toscana del 26 gennaio 2004, n. 1. Non è un dato irrilevante il ruolo centrale delle Regioni nell'amministrazione diretta di molti servizi pubblici come ricostruito recentemente nell'ampia monografia di G. Gardini, C. Tubertini, *L'amministrazione regionale*, Giappichelli, 2022, in particolare p. 391 dove le Regioni si caratterizzano per essere «enti titolari di compiti di legislazione e programmazione, chiamati, nelle materie di propria competenza, a disciplinare sia le funzioni, sia i servizi intestati a sé ed alle amministrazioni locali ed a programmarne ed organizzarne l'esercizio».

[97] Per tutti si vedano V. Bachelet, *Coordinamento*, in "Enciclopedia del diritto", vol. X, Giuffrè, 1962, p. 634; G. Sciullo, *L'organizzazione amministrativa*, Giappichelli, 2013 e la letteratura *ivi* richiamata; F. Cortese, *Il coordinamento amministrativo. Dinamiche e interpretazioni*, Franco Angeli, 2012. Il fenomeno è stato solitamente ricondotto «(i) ad una relazione organizzativa; (ii) all'esercizio di un potere avente ad oggetto di volta in volta rapporti organizzativi, piuttosto che l'agire amministrativo; (iii) al risultato delle suddette relazioni o azioni», così in S. Dettori, *Coordinamento e dovere d'ufficio nella logica dell'interdipendenza amministrativa*, in "P.A. Persona e Amministrazione", 2020, n. 1, pp. 21-50.

[98] Si veda sul punto C. Marzuoli, S. Torricelli (a cura di), *La dimensione sociale della contrattazione pubblica*, Editoriale Scientifica, 2017; da ultimo E. Caruso, *La funzione sociale dei contratti pubblici. Oltre il primato della concorrenza*, Jovene, 2022, dalle quali emerge un'eccedenza nella funzionalità dei contratti pubblici.

[99] G. Marongiu, *Il coordinamento come principio politico di organizzazione della complessità sociale*, in Id., "La democrazia come problema. Diritto, amministrazione ed economia", vol. 1, il Mulino, 1994, p. 181 ss.

[100] S. Dettori, *Coordinamento e dovere d'ufficio*, cit.

[101] *Ivi*, nota 1, con i richiami alla dottrina più autorevole (Berti, Cassese, Nigro).

[102] S. Dettori, *Coordinamento e dovere d'ufficio*, cit.

[103] In termini, richiamata da S. Dettori, *Coordinamento e dovere d'ufficio*, cit., p. 39; si veda A. Pioggia, *La competenza amministrativa. L'organizzazione tra specialità pubblicistica e diritto privato*, Giappichelli, 2001, in particolare p. 157 ss. dove l'A. considera la competenza «come compito di ponderazione fra l'interesse perseguito in via primaria e gli altri interessi tutelati dall'ordinamento, acquistando la dimensione dinamica di una forza propulsiva dell'azione amministrativa» (p. 178). Secondo l'A., dunque, la competenza deve considerarsi «non più soltanto come limite relativo alla dimensione del potere che ciascun ufficio può esprimere nell'azione esterna, ma principalmente come indicazione della direzione che quel potere deve seguire nel suo esercizio» (p. 185). L'attribuzione delle competenze, infatti, nell'originale teoria dell'A. non si ridurrebbe a un tassello della teoria dell'imputazione, cioè come il passaggio logico utile a collegare «alla capacità giuridica statale la capacità di agire dei suoi organi», costituendo piuttosto il «momento in cui l'astratto interesse diviene compito di un ufficio e, quindi, concreta doverosità nell'esercizio di una funzione ad esso attribuita della competenza» (pp. 180-181).

[104] S. Dettori, *Coordinamento e dovere d'ufficio*, cit., p. 41.

[105] *Ibidem*.

The algorithms within the public sector and their governance

Abstract: After quickly outlining the role of administrative law in the management of social complexity, the use of algorithms internally by public administrations are examined. In this first part the problems that algorithms have raised and the solutions that literature and jurisprudence have offered will be discussed. In a second step, however, to overcome the binarism between acceptance and rejection of the digitisation of administrative procedures, the topic is approached from a broader perspective, that of the 'public administration of algorithms'. In this perspective we examine the opportunity to interpret some provisions of the Italian Code of Digital Administration (CAD), such as software re-use, as instruments of IT coordination.

Keywords: Datafication – Public algorithm – Source code – Document access – CAD – Software reuse – Administrative coordination

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0093
Articolo sottoposto a peer review

Bisogni conoscitivi delle amministrazioni e principio di legalità: quale predeterminazione delle scelte conoscitive pubbliche?

Matteo Falcone

Il saggio indaga lo stretto rapporto che esiste tra il principio di legalità e le attività di identificazione e di soddisfazione dei bisogni conoscitivi delle amministrazioni. Un rapporto che si è evoluto nel tempo e che oggi, con lo sviluppo e il progressivo utilizzo dei big data e degli algoritmi nell'azione amministrativa, necessita di un nuovo assetto.

Algoritmi – Principio di legalità – Banche dati

Sommario: *1. Introduzione – 2. Le attività di identificazione e di soddisfazione dei bisogni conoscitivi pubblici – 3. Il duplice rapporto con il principio di legalità – 4. Il carattere implicito e informale delle attività conoscitive delle amministrazioni (e dei relativi poteri) nella legge sul procedimento – 5. La progressiva oggettivizzazione delle attività informative e conoscitive pubbliche: le regole sulle banche dati tra coordinamento delle scelte conoscitive e regole di circolazione dei dati pubblici – 6. Le tecnologie algoritmiche per identificare e soddisfare i bisogni conoscitivi delle amministrazioni pubbliche: potenzialità, rischi ed effetti sulla funzione informativa e conoscitiva – 7. La crisi del rapporto tra bisogni conoscitivi e principio di legalità e la necessità di pensare una più stringente predeterminazione normativa e amministrativa dell'utilizzo dei moduli conoscitivi algoritmici*

1. Introduzione

Negli ultimi anni la diffusione delle tecnologie algoritmiche nei processi decisionali ha coinvolto anche le amministrazioni pubbliche[1]. Queste ultime hanno cominciato ad utilizzare gli algoritmi e i big data nello svolgimento delle rispettive funzioni amministrative, in particolare per prendere direttamente e in modo automatico la decisione amministrativa[2], ma anche per produrre nuova conoscenza sui fenomeni sociali e naturali o sulle situazioni di fatto oggetto dell'azione amministrativa[3].

I modi attraverso i quali questo tipo di conoscenza viene sviluppata – come vedremo – producono effetti sui diritti fondamentali e sulla cura degli interessi collettivi in modo diretto e più marcato rispetto ai metodi e alle tecniche conoscitive tradizionali[4]. Per questo motivo il suo utilizzo nell'esercizio delle funzioni amministrative impone una riflessione approfondita sulla conoscenza pubblica oggi, sulle trasformazioni che stanno interessando i moduli conoscitivi delle amministrazioni e sulle prospettive future di questa importante funzione pubblica[5].

Tra le tante questioni che si possono indagare, in questo lavoro si cercherà di analizzare lo stretto rapporto che esiste tra il principio di legalità e l'identificazione e la soddisfazione dei bisogni conoscitivi delle amministrazioni. Un rapporto – come vedremo – che si declina su due versanti e che vede, da un lato, la soddisfazione di questi ultimi come il presupposto necessario per garantire il rispetto del principio di legalità (inteso sia in senso stretto, sia in senso più

M. Falcone è assegnista di ricerca in Diritto amministrativo (IUS/10) e docente di Diritto dell'informazione e della comunicazione presso il Dipartimento di Scienze politiche dell'Università degli studi di Perugia. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

largo) nell'azione amministrativa[6]. Dall'altro lato e in modo inverso, che vede la presenza di specifiche disposizioni normative dedicate all'identificazione e alla soddisfazione dei bisogni conoscitivi delle amministrazioni come il presupposto necessario per assicurare che l'utilizzo e l'organizzazione degli strumenti conoscitivi pubblici, soprattutto quelli di natura autoritativa, garantisca il pieno rispetto del principio di legalità durate l'esercizio delle funzioni amministrative.

Un rapporto che è tornato al centro delle riflessioni giuridiche, in particolare di quelle giuspubblicistiche, considerando che proprio la diffusione dei moduli conoscitivi algoritmici nell'azione delle amministrazioni e le trasformazioni che stanno apportando al modo di produrre conoscenza pubblica sta mettendo in evidenza l'inadeguatezza dell'attuale assetto normativo della funzione conoscitiva, sia rispetto ai bisogni conoscitivi delle amministrazioni, sia rispetto alle garanzie e alle tutele che l'utilizzo di strumenti tecnologici di questo tipo obbligano ad assicurare.

2. Le attività di identificazione e della soddisfazione dei bisogni conoscitivi pubblici

Prima di entrare nel merito di questi cambiamenti, è utile spiegare che cosa si intende per attività di identificazione e di soddisfazione dei bisogni conoscitivi delle amministrazioni pubbliche in questo lavoro.

La letteratura scientifica, non solo di provenienza giuridica, ha da moltissimo tempo messo in evidenza come l'azione amministrativa – nella sua duplice funzione di scelta (di composizione di interessi) e di garanzia (di tutela di posizioni giuridiche con il riconoscimento di diritti procedimentali) – deve basare le sue decisioni su elementi di razionalità, cioè sulla raccolta di elementi conoscitivi.

Questa prospettiva, che già Max Weber legava intimamente al fenomeno burocratico, è senz'altro una delle caratteristiche più antiche e tradizionali dell'azione amministrativa[7]. L'amministrazione pubblica, affermava Franco Levi alla fine degli anni Sessanta del secolo scorso, durante la sua azione concreta sviluppa una fondamentale attività «per conoscere la situazione di fatto, in senso lato sociale, in cui si trova ad operare», che costituisce un tratto specifico dell'azione pubblica in quanto attività "razionale"[8].

Le attività conoscitive delle amministrazioni, dunque, sono quelle attività che mirano a identificare e a soddisfare i bisogni di natura conoscitiva delle amministrazioni, cioè i bisogni che queste hanno di possedere dati, informazioni e conoscenze tecnico-scientifiche, sia per conoscere la realtà che amministrano e per orientare, sulla base di questa conoscenza, la decisione normativa o amministrativa generale, sia per applicarle nella decisione amministrativa puntuale, al fine di comporre nel migliore modo possibile l'interesse pubblico nel caso concreto[9].

Per fare qualche esempio, nel primo caso basti pensare alle attività volte alla conoscenza della realtà naturale (l'assetto idrogeologico di una regione; la previsione di una calamità) o alla conoscenza della realtà economica e sociale (la povertà; l'invecchiamento della popolazione). Nel secondo caso ci riferiamo alle attività di natura tecnico-scientifiche come la progettazione di un'opera pubblica; la misurazione di un fenomeno naturale, come l'inquinamento di un fiume o dell'aria; la progettazione, la programmazione o la gestione di un sistema informativo; infine, la prevenzione e la gestione di una pandemia.

In entrambi i casi le amministrazioni devono identificare i bisogni conoscitivi, cioè sapere individuare "che cosa bisogna conoscere", quali dati, informazioni e conoscenze bisogna avere per esercitare opportunamente determinate funzioni. Così come, una volta identificati, esse devono organizzarsi per soddisfare quei bisogni conoscitivi, devono predisporre il "come bisogna conoscere", come organizzarsi per raccogliere quei dati, quelle informazioni e quella conoscenza identificata come necessaria per esercitare determinate funzioni.

Queste attività, come avremo modo di specificare, sono spesso indirizzate dalla legge, in particolare quando questa – individuando le finalità e gli scopi – di fatto indica quali sono i bisogni conoscitivi che l'amministrazione deve soddisfare per il corretto svolgimento di una determinata funzione amministrativa. L'amministrazione, però, è chiamata spesso a fare un ulteriore sforzo di precisazione e di specificazione del bisogno conoscitivo concreto legato all'esercizio di quella determinata funzione amministrativa oppure si trova a scegliere autonomamente quali strumenti e quali regole organizzative darsi per ottenere quei dati, quelle informazioni e quella conoscenza.

3. Il duplice rapporto con il principio di legalità

Le attività di identificazione e di soddisfazione dei bisogni conoscitivi delle amministrazioni sono un aspetto spesso trascurato dalla dottrina e sottovalutato dal legislatore[10], nonostante abbiano uno stretto e duplice rapporto con il principio di legalità[11].

In primo luogo esse sono il presupposto necessario per assicurare il rispetto del principio di legalità nell'azione amministrativa inteso in senso stretto, cioè come rispetto del comando contenuto nelle norme.

L'analisi di determinati fenomeni, l'accertamento di un determinato fatto di realtà, il verificarsi di una determinata situazione che coinvolge l'interesse pubblico (e gli interessi secondari) molte volte costituisce il presupposto che giustifica l'attivazione di determinati poteri e procedure amministrative o di particolari interventi pubblici. La capacità delle amministrazioni di rappresentare e di ricostruire fenomeni, fatti di realtà e situazioni, dunque, è fondamentale per inquadrare nel modo più preciso possibile la fattispecie concreta nella fattispecie astratta presente nella legge, per condurre un'azione amministrativa davvero rispettosa del comando normativo, il quale diversamente sarebbe "svuotato" e disatteso[12].

Ma più in generale l'opportuna identificazione e la completa soddisfazione dei bisogni conoscitivi sono un presupposto indispensabile anche per assicurare una legalità dell'azione amministrativa intesa in senso più largo, che vada oltre la semplice verifica dell'inverarsi della fattispecie normativa nell'azione concreta e che sia orientata, invece, al perseguimento degli scopi costituzionali del fenomeno amministrativo, cioè alla piena emersione degli interessi coinvolti nella decisione, in particolare quelli a protezione necessaria, come indicato nell'articolo 97 della Costituzione, e la compiuta e universale tutela dei diritti individuali e sociali, così come indicato nell'articolo 3, comma 2 della Costituzione.

L'identificazione e la soddisfazione dei bisogni conoscitivi risultano essere uno dei fattori più rilevanti nella prospettiva dell'imparzialità *ex* art. 97 della Costituzione. L'imparzialità dell'azione amministrativa non deve essere vista solo sotto il profilo della non discriminazione della decisione, ma *in primis* come adeguata conoscenza della verità dei fatti e della realtà oggettiva delle cose, che significa per l'amministrazione interessata avere completa consapevolezza delle diverse posizioni – e dei diversi interessi che quelle posizioni rappresentano – coinvolte in una determinata decisione[13]. Molte volte ricostruire situazioni di fatto nel modo più preciso possibile, conoscere nel modo più oggettivo e completo possibile caratteri, cause ed effetti di un determinato fenomeno significa – nell'ottica della decisione – non solo garantire all'amministrazione un quadro conoscitivo che si avvicina alla realtà oggettiva delle cose, ma significa anche fare emergere il numero più alto possibile di interessi individuali o collettivi "nascosti", non ancora rappresentati all'interno della decisione, i quali fino a quel momento e per qualsiasi motivo non erano stati presi in considerazione dall'amministrazione o non avevano preso parte autonomamente alle dinamiche procedimentali.

La piena emersione degli interessi coinvolti nelle attività amministrative – in particolare quelli a protezione necessaria[14] – inoltre, non solo contribuisce a districare la complessità della realtà in cui le amministrazioni operano, ma permettono a queste ultime di organizzarsi e di predisporre tutti gli strumenti possibili per garantire i diritti sociali e individuali a tutte le persone, in particolare rimuovendo gli ostacoli di ordine economico e sociale che impediscono la piena realizzazione e il pieno sviluppo della persona, di cui parla l'articolo 3 comma 2 della Costituzione[15].

Questo versante del rapporto con il principio di legalità, anche di derivazione costituzionale – che presuppone una spinta delle amministrazioni verso la produzione di una conoscenza pubblica più completa possibile – si rafforza con lo sviluppo tecnologico nella società dell'informazione: tanto più la tecnologia allarga i confini della conoscenza possibile, tanto più le amministrazioni hanno il dovere di utilizzare ogni strumento per raggiungerla, anche di natura tecnologica.

Le attività di identificazione e di soddisfazione dei bisogni conoscitivi delle amministrazioni, dunque, sono fondamentali non solo per rendere la decisione amministrativa una decisione "giusta", cioè realmente imparziale e rispettosa del principio di stretta legalità, ma anche per concretizzare lo scopo profondo dell'azione delle amministrazioni come motore di trasformazione sociale contenuto nella Costituzione repubblicana.

Avendo chiaro l'importanza e il rilievo costituzionale di questo primo profilo del rapporto tra principio di legalità e attività di identificazione e di soddisfazione dei bisogni conoscitivi delle amministrazioni, è necessario cominciare a riflettere sull'altro versante di questo rapporto, cioè se e come la legge fornisce oggi poteri e strumenti alle amministrazioni pubbliche per identificare e per soddisfare i propri bisogni conoscitivi, al fine di permettere loro di garantire il pieno rispetto del principio di legalità nell'esercizio delle funzioni amministrative.

Questo secondo versante del rapporto tra bisogni conoscitivi e principio di legalità si è progressivamente irrobustito nel tempo e oggi necessita di un nuovo assetto, in particolare alla luce dei caratteri della conoscenza algoritmica e degli effetti che questa produce sull'azione delle amministrazioni.

4. Il carattere implicito e informale delle attività conoscitive delle amministrazioni (e dei relativi poteri) nella legge sul procedimento

Nonostante il loro pieno svolgimento costituisca una fondamentale garanzia di effettività del principio di legalità, le attività di identificazione e di soddisfazione dei bisogni conoscitivi per molto tempo non

sono emerse compiutamente nel diritto positivo. Tradizionalmente il legislatore (suffragato anche dalla elaborazione dottrinaria) ha sempre considerato le attività e i poteri conoscitivi delle amministrazioni come attività e poteri impliciti strumentali all'esercizio della funzione amministrativa, anche quando la norma non li prevedesse esplicitamente[16].

Solo con la legge sul procedimento amministrativo emerge nel diritto positivo un primo e rilevante riferimento normativo di carattere generale sulle attività conoscitive delle amministrazioni.

La legge 241 del 1990 non prevede regole direttamente collegabili alla individuazione e alla soddisfazione dei bisogni conoscitivi nel procedimento amministrativo ma, disciplinando i compiti del responsabile del procedimento, introduce alcuni principi generali (il principio di completezza e di adeguatezza dell'istruttoria, il principio inquisitorio con metodi acquisitivi, il principio di informalità, il principio di non aggravamento del procedimento) che tentano di fornire all'amministrazione la legittimazione, i poteri di scelta discrezionale e gli strumenti per avvicinarla il più possibile alla ricostruzione oggettiva dei fenomeni sociali, dei fatti o delle situazioni coinvolti nel procedimento, per spingerla alla "ricerca della verità", ovviamente materiale, delle cose[17].

Se guardiamo questi principi dal punto di vista degli strumenti e dei poteri che le amministrazioni pubbliche possono legittimamente utilizzare nelle loro attività conoscitive, il principio di completezza e di adeguatezza – non solo pone un obiettivo all'amministrazione e un parametro di legittimità della decisione al giudice amministrativo (una conoscenza istruttoria completa e adeguata, appunto) – ma legittima e quasi spinge le amministrazioni pubbliche ad utilizzare tutti gli strumenti possibili in quel dato momento storico, per ricostruire in modo adeguato e completo i fenomeni, i fatti o le situazioni oggetto di un intervento pubblico o di un determinato procedimento amministrativo.

Secondo lo schema della legge sul procedimento, inoltre, il *modus operandi* delle amministrazioni che vogliono soddisfare i loro bisogni conoscitivi è prevalentemente retto dal principio di informalità e dal principio inquisitorio. Tali principi permettono alle amministrazioni di adottare – anche al di là di una specifica norma legittimante – atti, anche di natura autoritativa, con il fine di costruire una rappresentazione delle cose corrispondente alla natura dei fenomeni così come presenti nella realtà (con un grado di approssimazione che sia ritenuto accettabile nel caso concreto), di precisare concetti che sono inizialmente a contenuto variamente indeterminato e, infine, di chiarire fatti di una certa complessità[18].

Nella legge sul procedimento, in sintesi, l'attività conoscitiva delle amministrazioni è una attività prevalentemente informale che, al fine di raggiungere una conoscenza adeguata e completa dei fatti, garantisce al responsabile del procedimento un ventaglio di possibili strumenti e poteri che può utilizzare discrezionalmente, anche poteri autoritativi di tipo inquisitorio, che, attraverso l'utilizzo concreto dei moduli conoscitivi e acquisitivi, può toccare i diritti individuali delle persone e gli interessi collettivi. Ovviamente all'interno del procedimento l'invasività di tale potere conoscitivo viene bilanciato da altre esigenze (come quella della ragionevole durata del procedimento) e limitato da adeguate garanzie procedimentali, che crescono al crescere di tale potere, in particolare all'interno di particolari settori dell'amministrazione, come l'amministrazione finanziaria.

Nella disciplina sul procedimento amministrativo, dunque, il rapporto tra le attività di identificazione e di soddisfazione dei bisogni conoscitivi e il principio di legalità si è concentrato, da un lato, sulla definizione di principi metodologici per svolgerle (i principi di completezza, adeguatezza, informalità e inquisitorio, non aggravamento), alcuni dei quali costituiscono importanti parametri di legittimità dell'istruttoria, e, dall'altro lato, sulle garanzie procedimentali quando queste attività assumono un carattere autoritativo. Molto meno sulle scelte conoscitive concrete delle amministrazioni, lasciate alla discrezionalità del responsabile del procedimento (quali dati e informazioni raccogliere; quali conoscenze acquisire) e alla sua capacità di ricavarle direttamente dalle finalità della funzione amministrativa individuate dalla legge.

5. La progressiva oggettivizzazione delle attività informative e conoscitive pubbliche: le regole sulle banche dati tra coordinamento delle scelte conoscitive e regole di circolazione dei dati pubblici

Con la progressiva informatizzazione e digitalizzazione pubblica, il rapporto tra attività di identificazione e soddisfazione dei bisogni conoscitivi e il principio di legalità cambia e si irrobustisce notevolmente.

In questo contesto le amministrazioni pubbliche divengono, molto più di prima[19], degli importanti soggetti informativi, cioè dei soggetti che nello svolgimento delle proprie attività raccolgono, conservano e analizzano i dati, li trasformano in informazioni per produrre conoscenza e, sulla base di questa, prendere decisioni o fornire beni e servizi[20].

La diffusione della logica dei dati in luogo della logica dei documenti e la progressiva importanza acquisita dal patrimonio informativo pubblico, inoltre, rendono le attività di identificazione e soddisfazione dei bisogni conoscitivi delle amministrazioni attività autonome rispetto alle dinamiche procedimentali: emerge una vera e propria funzione informativa e conoscitiva, con proprie regole e propri apparati con cui/in cui i dati e le informazioni vengono raccolte (prevalentemente con l'attività procedimentale, ma non solo) e utilizzate più volte, non solo dalla stessa amministrazione che le ha raccolte, ma anche da tutto il sistema amministrativo nonché dai cittadini e dalle imprese[21]. In questa funzione amministrativa emergente, l'organizzazione dei dati e delle informazioni all'interno di banche dati diviene il carattere distintivo e la loro formazione e la loro condivisione/fruizione diventa il principale strumento di soddisfazione dei bisogni conoscitivi del sistema amministrativo, nonché il principale modulo conoscitivo nella decisone amministrativa concreta delle singole amministrazioni[22].

In questo contesto, che qui abbiamo ricostruito solo in sommi capi, il rapporto tra attività di identificazione e di soddisfazione dei bisogni conoscitivi e principio di legalità assume nuove forme, più robuste rispetto al periodo precedente: emerge, infatti, una prima attenzione del legislatore sia verso le attività di identificazione dei bisogni conoscitivi, sia verso la predisposizione di strumenti e poteri utili per la loro soddisfazione, che si concretizza attraverso la disciplina delle banche dati come strumenti conoscitivi, ancora prevalentemente "statici", di conservazione e di organizzazione ragionata dei dati e delle informazioni.

In primo luogo il legislatore prevede per la prima volta delle regole sull'identificazione e sulla soddisfazione dei bisogni conoscitivi comuni a tutto il sistema amministrativo, declinate nel concreto come scelte di coordinamento di alcune basi di dati, che già erano nate e formate a livello di singola amministrazione, per migliorare la fruibilità e l'efficacia dell'azione amministrativa all'interno di determinate funzioni amministrative. Ci riferiamo alle norme sulle basi di dati di interesse nazionale[23], diretta declinazione del potere di «coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale» *ex* art. 117, comma 2, lett. r), Cost.[24] Nell'esercizio di questa competenza repubblicana è possibile per lo Stato vincolare tutti i livelli di governo ad indicazioni comuni non soltanto con riferimento alle modalità di gestione tecnica del patrimonio informativo pubblico (il coordinamento tecnico a fini statistici e informatici), ma anche relativamente alle scelte conoscitive e ai loro trattamenti (coordinamento informativo)[25]. Le basi di dati di interesse nazionale, però, non sono stabilite per legge una volta per tutte: considerando che nel tempo potrebbero sorgere all'interno del sistema amministrativo nuovi bisogni conoscitivi (la creazione di nuove basi di dati) o nuove esigenze di coordinamento informativo (la condivisione di altre basi di dati esistenti), il Codice dell'amministrazione digitale (CAD) assegna all'Agenzia per l'Italia Digitale (AgID) la possibilità di individuare ulteriori basi di dati di interesse nazionale, oltre quelle presenti nel testo normativo[26].

Dopo il d.l. 31 maggio 2021, n. 77, che ha modificato l'art. 50-*ter* del CAD, si è fatto un passo ulteriore in termini di condivisione dei dati. Questa disposizione ha reso la Piattaforma Digitale Nazionale Dati (PDND) lo strumento principale di accesso, di condivisione e di utilizzo dei dati pubblici detenuti dalle amministrazioni[27]. La PDND è attualmente il luogo principale (un vero e proprio *data lake*), centralizzato e controllato dalla Presidenza del Consiglio dei ministri, all'interno del quale devono confluire tutti i dati pubblici la cui condivisione è ritenuta determinante per il corretto svolgimento delle funzioni amministrative, a partire dai dati contenuti nelle basi di dati di interesse nazionale[28].

Oltre a queste prime regole, il legislatore rafforza la prospettiva della soddisfazione dei bisogni conoscitivi delle amministrazioni attraverso tre ulteriori nuclei di norme sulla circolazione dei dati e delle informazioni nel sistema amministrativo e, più in generale, nella società.

Il primo nucleo di tali regole è quello sulla fruibilità dei dati, da non intendersi più come mera possibilità per una amministrazione di accedere previa autorizzazione alla banca dati di un'altra amministrazione, ma come la possibilità di utilizzare direttamente il dato (accedendo direttamente e gratuitamente alla banca dati delle altre amministrazioni) e anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione[29]. Il secondo nucleo è quello sull'adozione nel nostro ordinamento dei requisiti internazionali di qualità dei dati. Tali requisiti trovano riscontro in una serie di principi di carattere trasversale, riferiti sia alle modalità tecniche di gestione dei dati in formato elettronico (esattezza, disponibilità, accessibilità, integrità e riservatezza, vedi art. 51 CAD) sia alle caratteristiche tecniche dei siti destinati ad assicurarne la fruizione e la diffusione al pubblico (usabilità e reperibilità, completezza, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità[30]. Il terzo nucleo riguarda la diffusione delle informazioni fuori dal sistema amministrativo e le regole sulla circolazione e sulla protezione dei dati personali. La filosofia degli open data e la sua declinazione italiana, contenuta nel d.lgs. 14 marzo 2013, n.

33, ha reso i dati pubblici – in modo particolare quelli legati agli obblighi di pubblicazione contenuti nel Codice della trasparenza – aperti, disponibili per tutti in formato aperto e riutilizzabili. L'intento profondo della diffusione dei dati pubblici è di natura conoscitiva: in primo luogo quello di contribuire alla formazione della conoscenza collettiva, ma anche quello di favorire un ritorno conoscitivo nelle amministrazioni, attraverso la partecipazione di coloro che hanno utilizzato e rielaborato i dati pubblici alla decisione pubblica[31]. In un contesto di libera circolazione (o quasi) dei dati pubblici dentro e fuori il sistema amministrativo e fuori da un contesto "protetto" come il procedimento amministrativo, in ultimo, le regole sul trattamento dei dati personali rappresentano l'unica forma di garanzia per le persone coinvolte dalla raccolta, conservazione e diffusione dei dati. I principi sulla riservatezza dei dati personali, in ultimo contenuti nel Regolamento UE 2016/679, hanno sempre avuto come obiettivo quello di favorire una circolazione e un trattamento corretto di questi dati, ma hanno sempre scoraggiato la concentrazione dei dati in un'unica banca dati, incentivando la frammentazione della conservazione dei dati[32].

Nella società dell'informazione, dunque, identificare e soddisfare i bisogni conoscitivi delle amministrazioni significa, da un lato, individuare nello specifico le banche dati da coordinare e da condividere nel sistema amministrativo (le basi di dati di interesse nazionale), attuando direttamente o interpretando autonomamente l'indirizzo legislativo sulle finalità della funzione (che identifica i bisogni conoscitivi in via generale) e, dall'altro lato, facilitare il più possibile la circolazione dei dati pubblici (garantendo la protezione dei dati personali) nel e fuori il sistema amministrativo.

Rispetto al rapporto che si è cristallizzato nelle attività conoscitive procedimentali, basato solo su una disciplina "metodologica" (relativa alla soddisfazione dei bisogni conoscitivi), senza alcun indirizzo specifico sulla loro identificazione, nella funzione conoscitiva e informativa pubblica il rapporto tra bisogni conoscitivi e principio di legalità sembra ispessirsi e spostarsi prevalentemente sul piano organizzativo, sull'identificazione dei bisogni conoscitivi, in particolare grazie alla presenza delle norme sulle banche dati pubbliche, sulla circolazione dei dati pubblici, e sulla circolazione dei dati pubblici come strumento di ulteriore soddisfazione dei bisogni conoscitivi.

Un quadro che non manca di contraddizioni e di appesantimenti. La contraddizione principale è quella che abbiamo anche segnalato poco sopra: se, da un lato, le norme sulla formazione e sull'utilizzo delle banche dati di interesse nazionale tendono verso la costituzione di un grande *data lake* pubblico come la PDND, dall'altro lato, le norme sulla protezione dei dati personali tendono a ridimensionarne la portata, soprattutto se si tratta di condividere dati di natura personale. Una contraddizione che, però, sembra oramai superata dallo stesso legislatore con le recenti modifiche al Codice della privacy[33]. Il legislatore, abrogando i poteri preventivi del Garante sui trattamenti effettuati dalle amministrazioni pubbliche e aggiungendo l'atto amministrativo generale alle altre basi giuridiche che legittimano il trattamento dei dati personali, ha di fatto facilitato l'utilizzo dei dati personali nell'esercizio delle funzioni pubbliche.

L'appesantimento, invece, deriva dall'atteggiamento del legislatore relativamente alla costruzione delle banche dati di interesse nazionale. Quest'ultima si è declinata spesso come moltiplicazione di oneri informativi in capo alle singole amministrazioni, le quali erano costrette ad inviare i medesimi dati a più amministrazioni, aggravandole di oneri che sarebbero stati facilmente superabili con una maggiore interoperabilità delle banche dati. È il caso, ad esempio, dell'invio dei dati e delle informazioni relative ai contratti pubblici, la cui onerosità ha costretto il legislatore ad introdurre il principio di unicità del luogo di pubblicazione e di unicità dell'invio delle informazioni all'interno del Codice dei contratti[34], al fine di semplificare l'invio dei dati sulle aggiudicazioni e sulle esecuzioni dei contratti da parte delle singole amministrazioni.

6. Le tecnologie algoritmiche per identificare e soddisfare i bisogni conoscitivi delle amministrazioni pubbliche: potenzialità, rischi ed effetti sulla funzione informativa e conoscitiva

Oggi questo rapporto, rafforzatosi negli ultimi anni nel senso che abbiamo descritto, si sta lentamente trasformando ed allentando con il progressivo utilizzo dei c.d. big data, degli algoritmi e del loro potere computazionale nell'azione amministrativa[35].

Queste tecnologie hanno caratteristiche molto precise: sono capaci di produrre, di raccogliere e di conservare massivamente ed in tempo reale dati eterogenei; sono in grado di elaborare i dati in modo massivo, anche incrociando banche dati differenti, con una potenza di calcolo senza precedenti; i sistemi di intelligenza artificiale, in particolare, permettono anche di semplificare i processi decisionali, in quanto sono capaci sia di razionalizzare le opzioni di scelta che bisogna valutare relativamente ad una particolare decisione, le quali tradizionalmente richiederebbero uno sforzo di elaborazione dei dati molto gravoso per l'uomo, sia di prendere direttamente e autonomamente le decisioni[36].

La conoscenza algoritmica, basata su correlazioni statistiche, non ha come obiettivo quello di spiegare la realtà con analisi causa-effetto, ma solo quello di fare emergere – attraverso delle correlazioni statistiche che legano variabili tra loro – connessioni che non erano facilmente visibili all'operatore. Tali connessioni, da un lato, fanno emergere fenomeni che sono già presenti nel tessuto economico e sociale, ma che non era possibile osservare con l'impostazione analitica tradizionale (attraverso mappature, profilazioni, categorizzazioni, classificazioni, correlazioni), dall'altro lato, possono mostrare previsioni probabilistiche sull'andamento dei fenomeni in analisi, con margini di errore più o meno rilevanti[37]. Questo tipo di conoscenza ha rinnovato l'attenzione generale sulla centralità dei dati, delle informazioni e della conoscenza nella decisione amministrativa. Considerando la crescente complessità del contesto normativo e sociale in cui le amministrazioni si trovano ad operare, la crescita progressiva dei diritti e degli interessi che le amministrazioni sono chiamate a garantire o a curare, la conoscenza algoritmica e la sua capacità di allargare e arricchire in modo non scontato le prospettive conoscitive delle amministrazioni sui diritti e sugli interessi coinvolti dalla decisione può essere un fattore importante per l'identificazione di nuovi bisogni conoscitivi e per la loro complessiva soddisfazione, oltre che per il miglioramento della funzionalità, dell'imparzialità e dell'efficacia dell'azione amministrativa quotidiana (e per una maggiore conciliazione con le necessità conoscitive)[38].

Queste potenzialità, in modo particolare, da un lato, stanno rafforzando le esigenze di circolazione e di fruibilità dei dati pubblici nel sistema amministrativo e, dall'altro, stanno facendo emergere la necessità di elaborare i dati in possesso delle amministrazioni attraverso l'integrazione sistematica delle banche dati pubbliche. Tale necessità, fino ad oggi presente solo marginalmente nelle amministrazioni pubbliche, sta emergendo nelle prassi amministrative di molte amministrazioni, in particolare all'interno dei grandi enti pubblici nazionali e delle autorità amministrative indipendenti[39]. Questo aspetto sta trasformando il ruolo e le funzioni delle banche dati: da strumento conoscitivo statico (frutto di una riorganizzazione ragionata delle informazioni) e di garanzia (di qualità dei dati e di protezione di quelli personali) a potenziale strumento conoscitivo dinamico e integrabile, di elaborazione massiva di dati differenti al fine di produrre nuova conoscenza algoritmica. D'altronde, anche la stessa PDND non è stata solo pensata per fungere da *data lake* pubblico per condividere e fare circolare dati pubblici, ma anche per utilizzarne le potenzialità conoscitive delle loro elaborazioni algoritmiche[40].

Un tipo di conoscenza e delle tendenze trasformatrici che – oltre alle potenzialità e ai vantaggi conoscitivi – ha mostrato anche rischi e incertezze quando è stata utilizzata nelle amministrazioni. Si pensi ai rischi per la protezione dei dati personali dovuti ai metodi massivi e invasivi di raccolta ed elaborazione dei dati per produrre questo tipo di conoscenza, in particolare quando vengono utilizzati dati personali; all'opacità del funzionamento degli algoritmi nelle elaborazioni conoscitive; alle distorsioni a cui possono essere soggetti i risultati delle elaborazioni algoritmiche a causa di errori in fase di costruzione del *dataset*, di progettazione dell'algoritmo o – nei casi di sistemi di *machine learning* o *deep learning* – durante la fase di apprendimento autonomo dell'algoritmo, che possono portare ad una conoscenza parziale o fallace della realtà e, dunque, a conseguenze discriminatorie o a decisioni ingiuste, fondate su una base conoscitiva distorta; infine al rischio di "cattura" del decisore da parte dei risultati algoritmici, cioè il rischio di affidarsi largamente ai risultati delle elaborazioni algoritmiche e di restarne poi prigionieri, nella convinzione che questi possano produrre una decisione imparziale e neutra proprio perché al riparo dalla discrezionalità del fattore umano[41].

Siamo in presenza, dunque, di strumenti di identificazione e di soddisfazione dei bisogni conoscitivi il cui semplice utilizzo ha degli effetti diretti sui diritti individuali delle persone e sugli interessi collettivi, di una funzione conoscitiva e informativa che vede crescere moltissimo la componente del potere conoscitivo. In questo contesto, aspetti che prima erano considerati marginali o meramente tecnico-pratici (l'individuazione e la selezione delle basi di dati da incrociare; i criteri di elaborazioni e le istruzioni algoritmiche; la verifica e la valutazione dei risultati algoritmici) – e che di fatto non sono regolati da norme specifiche – diventano il fulcro della scelta conoscitiva delle amministrazioni, che in presenza di sistemi di intelligenza artificiale si spinge addirittura ad influire direttamente sulla decisione amministrativa.

7. La crisi del rapporto tra bisogni conoscitivi e principio di legalità e la necessità di pensare una più stringente predeterminazione normativa e amministrativa dell'utilizzo dei moduli conoscitivi algoritmici

Dalla ricostruzione che abbiamo compiuto in queste pagine, è evidente come l'utilizzo della conoscenza algoritmica, in particolare nell'azione amministrativa, impone di ripensare il rapporto tra identificazione

e soddisfazione dei bisogni conoscitivi e principio di legalità – basato sostanzialmente sulle regole "metodologiche" contenute nella legge sul procedimento amministrativo e sulle regole di coordinamento e di circolazione dei dati (con la protezione dei dati personali) –. Questo assetto normativo non è capace né di permettere un adeguato sviluppo delle potenzialità conoscitive algoritmiche, né di frenarne le implicazioni più rischiose per i diritti individuali, quando i sistemi di intelligenza artificiale vengono utilizzati direttamente nell'azione amministrativa. La domanda che ci si pone, allora, è quale assetto normativo è necessario costruire per fare sì che le attività di identificazione e di soddisfazione dei bisogni conoscitivi, condotte con la conoscenza algoritmica, assicurino l'effettività del principio di legalità, sia in senso stretto, sia in un senso più ampio.

Dall'analisi del diritto positivo emerge una prima risposta a questa esigenza, che mira a regolare principalmente la decisione algoritmica, cioè l'utilizzo delle tecnologie algoritmiche per prendere direttamente e automaticamente la decisione amministrativa[42], ma anche aspetti più organizzativi legati alla conoscenza algoritmica, che qui saranno brevemente evidenziati.

Si pensi a livello internazionale alla *Raccomandazione sull'etica dell'IA*, approvata il 24 novembre 2021 da tutti gli Stati membri durante la quarantunesima conferenza generale dell'UNESCO. Essa prevede principi che sono pensati principalmente per la decisione algoritmica, ma che si possono applicare anche alla gestione delle banche dati: ad esempio, il principio di proporzionalità e il principio di non nuocere, da intendersi come elaborazione e integrazione proporzionata delle banche dati, oltre che come divieto di costruzione di banche dati per costruire sistemi di punteggio sociale; il principio di equità e di non discriminazione, cioè costruire di banche dati senza *bias* etnici, religiosi, sociali, politici; il principio di protezione della privacy e dei dati personali, da leggersi come *privacy by design* e *by default*; il principio di trasparenza dell'IA e il diritto alla spiegazione della logica algoritmica, riferibile alla cura delle fasi di input, di output e, in generale del funzionamento dell'algoritmo e del modo in cui produce i risultati; infine, il principio di responsabilità e di *accountability*, declinabile in termini organizzativi come previsione di adeguati meccanismi di supervisione, di valutazione d'impatto, di audit e di *due diligence*.

Oppure nell'ordinamento europeo ad alcune disposizioni del regolamento sui dati personali – oltre al diritto alla spiegazione, che indirettamente rende *accountable* le scelte relative alla predisposizione del *dataset* e dell'algoritmo per l'elaborazione successiva[43] – che obbliga il titolare del trattamento che ricorre in via eccezionale ad una decisione unicamente basata sul trattamento automatizzato dei dati ad attuare tutte le misure «appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato». Le misure a cui questa disposizione fa riferimento sono prevalentemente misure organizzative che riguardano la gestione dei dati e delle banche dati: la valutazione di impatto, i controlli di garanzia e di qualità del trattamento, le procedure di audit degli algoritmi, la minimizzazione, la pseudonimizzazione e l'anonimizzazione dei dati personali che si intendono utilizzare e, infine, i meccanismi di certificazione[44].

Anche la proposta di regolamento sull'IA dedica l'art. 10, comma 3 alla selezione e alla cura dettagliata dei set dei dati che vengono utilizzati per l'addestramento, per la convalida e per la prova dei sistemi di IA. Il regolamento individua a questo fine una serie di momenti in cui è necessaria una particolare attenzione da parte del fornitore nella gestione dei dati[45] al fine di ottenere un set di dati «pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi»[46].

Infine, è opportuno segnalare che anche il giudice amministrativo, nelle numerose sentenze sulla decisione algoritmica in cui ha individuato i primi principi sulla legalità algoritmica[47], afferma esplicitamente che la trasparenza della decisione algoritmica «deve essere garantita *in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti.* Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato»[48]. Anche il principio della supervisione umana e quello di non discriminazione, secondo il giudice amministrativo, presuppongono un intervento sulla gestione dei dati e sulla predisposizione dei *dataset* ai fini della loro elaborazione in quanto «il ricorso all'algoritmo va correttamente inquadrato *in termini di modulo organizzativo, di strumento procedimentale ed istruttorio*, soggetto alle verifiche tipiche di ogni procedimento amministrativo, il quale resta il modus operandi della scelta autoritativa, da svolgersi sulla scorta della legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico, titolare del potere»[49].

Questa ricostruzione ci dimostra come l'utilizzo dei dati, i criteri di integrazione delle banche dati, le regole sulla loro trasparenza e visibilità esterna, dunque, sono progressivamente oggetto di maggiore attenzione normativa e confermano come il rapporto tra identificazione e soddisfazione dei bisogni conoscitivi e il principio di legalità sia ancora debole, concentrato prevalentemente su uno specifico aspetto, sulla decisione automatizzata algoritmica, ma che progressivamente si stia spostando in modo più marcato verso una maggiore responsabilizzazione (anche) delle amministrazioni sulla gestione organizzativa dei metodi conoscitivi algoritmici.

Un elemento importante, ma che non sembra ancora sufficiente. Le potenzialità conoscitive dell'utilizzo degli algoritmi nella pubblica amministrazione e anche la necessità di regolarlo per mitigarne i rischi richiedono non solo di responsabilizzare maggiormente le amministrazioni pubbliche, ma anche una più stringente predeterminazione delle attività di identificazione e di soddisfazione dei bisogni conoscitivi con metodi algoritmici, declinando i principi generali che abbiamo richiamato poc'anzi e tarandoli meglio sull'azione amministrativa.

Una più stringente predeterminazione normativa e amministrativa dell'utilizzo dei moduli conoscitivi algoritmici è necessaria non solo per utilizzare al meglio la conoscenza algoritmica, ma come più generale strumento di crescita della cultura del dato, dell'informazione e del decidere conoscendo all'interno delle amministrazioni e dell'effettività del principio di legalità.

Note

[1]La letteratura amministrativistica recentemente si è occupata moltissimo del tema. Per tutti si v. AA.VV., *Amministrazione, responsabilità, giurisdizione*, Volume II, in A. Pajno, F. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", il Mulino, 2022; R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, University Press, 2021; G. Pesce, *Funzione amministrativa, intelligenza artificiale, blockchain*, Editoriale Scientifica, 2021. Per una prospettiva più generale sulla digitalizzazione, con un approfondimento su questi temi si v. B. Marchetti, *Amministrazione digitale*, in "Enciclopedia del diritto. Funzioni amministrative", 2022, p. 75 e ss.; E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in "Diritto pubblico", 2019, n. 2, pp. 363-391.

[2]Sulla decisione algoritmica si v. A. Masucci, *L'automatizzazione delle decisioni amministrative algoritmiche fra "big data" e "machine learning". Verso l'"algocratic governance"?*, in "Diritto e processo amministrativo", 2022, n. 2, pp. 265-313; G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intelligibilità*, Editoriale scientifica, 2019; L. Previti, *La decisione amministrativa robotica*, Editoriale scientifica, 2022; V. Brigante, *Evolving pathways of administrative decisions. Cognitive activity and data, measures and algorithms in the changing administration*, Editoriale scientifica, 2019; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in "Diritto pubblico", 2019, n. 1, p. 5 ss.; E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2, pp. 273-304.

[3]Sulla produzione di conoscenza algoritmica si v. M. Falcone, *Public Knowledge, Information Function and the Administration of Complexity*, in F. Di Lascio, M. De Donno (eds.), "Public Authorities and Complexity. An Italian Overview", Editoriale scientifica, in corso di pubblicazione.

[4]Hanno indagato sul rapporto tra tecnologie algoritmiche e diritti fondamentali A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, in "Rivista trimestrale di diritto pubblico", 2019, n. 4, p. 1171 ss.; G. De Minico, *Fundamental rights, European digital regulation and algorithmic challenge*, in "MediaLaws", 2021, n. 1, pp. 9-38; D. Martire, *Intelligenza artificiale e Stato costituzionale*, in "Diritto pubblico", 2022, n. 2, pp. 397-444.

[5]Sui cambiamenti e sulle questioni relative alla gestione dei dati e della conoscenza alla luce dei nuovi fenomeni tecnologici si v. G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2017; M. Falcone, *"Big data" e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in "Rivista trimestrale di diritto pubblico", 2017, n. 3, pp. 601-639. In via generale sulla funzione conoscitiva si v. M.P. Guerra, *Funzione conoscitiva e pubblici poteri*, Giuffrè, 1996; F. Merloni (a cura di), *L'informazione delle pubbliche amministrazioni*, Maggioli, 2002; E. Carloni, *Le verità amministrative. L'attività conoscitiva pubblica tra procedimento e processo*, Giappichelli, 2011.

[6]Un approccio al principio di legalità ripreso a partire dalle considerazioni svolte da M. Vogliotti, *Legalità*, in "Annali dell'Enciclopedia del diritto", VI, Giuffrè, 2013, pp. 371-435. In senso differente si v. per tutti G. Corso, *Tra legge e fattispecie: la prospettiva del diritto amministrativo*, in "Ars Interpretandi", 2019, n. 1, pp. 71-90.

[7]Così analizzava l'azione delle amministrazioni M. Weber, *Economia e società* (trad. it. T. Bagiotti), Giuffrè, vol. 2, 1961, p. 289.

[8]La citazione nel testo e questo approccio allo studio dell'attività conoscitiva delle amministrazioni appartiene a F. Levi, *L'attività conoscitiva della pubblica amministrazione*, Giappichelli, 1967.

[9]Questa definizione di bisogni conoscitivi è ispirata a partire dalle considerazioni presenti in F. Merloni, *Le attività conoscitive e tecniche delle amministrazioni pubbliche. Profili organizzativi*, in "Diritto pubblico", 2013, n. 2, pp. 481-520. Su questo tema più di recente anche C. Cudia, *Pubblica amministrazione e valutazioni tecniche: profili organizzativi*, in "Diritto pubblico", 2016, n. 1, pp. 1-36.

[10]Soprattutto quando quest'ultimo riduce o elimina questo tipo di attività attraverso le riforme di semplificazione dei procedimenti amministrativi. Per un approccio critico alle riforme di semplificazione si v. P. Piras, *Semplificazioni e buon andamento della Pubblica amministrazione. Tra Scilla e Cariddi: rispettare la complessità superando le complicazioni*, in "DPCE online", 2021, n. 2, pp. 1923-1943; M. Bombardelli, *Semplificazione normativa e complessità del diritto amministrativo*, in "Diritto pubblico", 2015, n. 3, pp. 985-1063.

[11]Sul principio di legalità in generale restano fondamentali G. Zanobini, *L'attività amministrativa e la legge*, in Id., "Scritti vari di diritto pubblico", Giuffrè, 1955; M.S. Giannini, *Diritto amministrativo*, in "Enciclopedia del diritto", 1964; F. Satta, *Principio di legalità e pubblica amministrazione nello Stato democratico*, Cedam, 1969; S. Fois, *Legalità (principio di)*, in

"Enciclopedia del diritto", 1973; C. Marzuoli, *Principio di legalità e attività di diritto privato della pubblica amministrazione*, Giuffrè, 1982; L. Carlassare, *Legalità (principio di)*, in "Enciclopedia giuridica", 1990; G. Corso, *In che senso il diritto positivo costituisce un vincolo per il giurista*, in G. Zaccaria (a cura di), "Diritto positivo e positività del diritto", Giappichelli, 1991; R. Guastini, *Legalità (principio di)*, in "Digesto delle discipline pubblicistiche", vol. IX, Utet, 1994, pp. 84-97; A. Travi, *Giurisprudenza amministrativa e principio di legalità*, in "Diritto pubblico", 1995, n. 1, p. 92; N. Bassi, *Principio di legalità e poteri amministrativi impliciti*, Giuffrè, 2001; M. Magri, *La legalità costituzionale dell'amministrazione. Ipotesi dottrinali e casistica giurisprudenziale*, Giuffrè, 2002; F. Merusi, *Sentieri interrotti della legalità*, il Mulino, 2007; *Il principio di legalità nel diritto amministrativo che cambia*, Atti del LIII Convegno di studi di scienza dell'amministrazione, Giuffrè, 2008; F. Merusi, *La legalità amministrativa. Altri sentieri interrotti*, il Mulino, 2012; G. Corso, *Principio di legalità e interpretazione della legge*, Editoriale Scientifica, 2014.

[12]F. Merloni, *Istituzioni di diritto amministrativo*, Giappichelli, 2022.

[13]U. Allegretti, *L'imparzialità amministrativa*, Cedam, 1965 e G. Pastori, *Principi costituzionali sull'amministrazione e principio inquisitorio nel procedimento*, in M. Cammelli, M.P. Guerra (a cura di), "Informazione e funzione amministrativa", Rimini, 1997.

[14]Sugli interessi a protezione necessaria si v. G. Rossi, *Principi di diritto amministrativo*, Giappichelli, 2022, p. 37.

[15]Sull'importanza dell'organizzazione come garanzia di tutela degli interessi e dei diritti si v. M. Nigro, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Giuffrè, 1966, p. 126; M.S. Giannini, *In principio sono le funzioni*, in "Amministrazione civile", 1957, n. 1; F. Merloni, *Organizzazione amministrativa e garanzie dell'imparzialità. Funzioni amministrative e funzionari alla luce del principio di distinzione tra politica e amministrazione*, in "Diritto pubblico", 2009, p. 57 ss.; G. Rossi, *Principi di diritto amministrativo*, cit. Recentemente anche E. Carloni, *Diritti by design. Considerazioni su organizzazione, autonomia organizzatoria e protezione degli interessi*, in "P.A. Persona e Amministrazione", 2020, n. 1, p. 51 ss. Per una prospettiva costituzionalmente orientata del ruolo dell'amministrazione si v. i contributi contenuti in AA.VV., *La necessaria discontinuità. Immagini del diritto pubblico*, il Mulino, 1990.

[16]Emblematico di questo approccio dottrinario è O. Ranelletti, *Le inchieste amministrative secondo il nostro diritto pubblico vigente*, in "Archivio di diritto pubblico", 1902, vol. 1, p. 166 ss., ma esso emerge anche nella ricostruzione dottrinaria precedente compiuta in F. Levi, *L'attività conoscitiva*, cit. e N. Bassi, *Principio di legalità*, cit.

[17]Per le riflessioni su procedimento amministrativo e "ricerca della verità" si v. E. Carloni, *Le verità amministrative*, cit.

[18]Si pensi a moduli conoscitivi procedimentali come le acquisizioni di scienza, le ispezioni, gli acclaramenti, le richieste documentali, gli accessi interamministrativi, le richieste di pareri e di valutazioni tecniche, gli studi scientifici. Sulle attività conoscitive procedimentali, oltre che F. Levi, *L'attività conoscitiva*, cit., si v. F. Merloni, *Attività conoscitive delle amministrazioni pubbliche e statistica ufficiale. Problemi organizzativi e funzionali*, in "Rivista trimestrale di diritto pubblico", 1994; M.T. Serra, *Contributo ad uno studio sulla istruttoria nel procedimento amministrativo*, Giuffrè, 1991; E. Cardi, *La manifestazione di interessi nei procedimenti amministrativi*, Maggioli, vol. 1, 1983; R. Perez, *L'istruzione nel procedimento amministrativo*, in "Rivista trimestrale di diritto pubblico", 1966, n. 3; M. De Benedetto, *Istruttoria amministrativa e ordine del mercato*, Giappichelli, 2008; E. Carloni, *Le verità amministrative. L'attività conoscitiva pubblica tra procedimento e processo*, Giuffrè, 2011. Recentemente sui corpi tecnici e sulle valutazioni tecniche a trent'anni dall'approvazione della legge sul procedimento si v. i contributi di A. Pajno, T. Bonetti, G. Torelli, G. Piperata, E. Guarnieri, M. Cammelli, in A. Bartolini, B. Marchetti, B.G. Mattarella et al. (a cura di), *La legge n. 241 del 1990, trent'anni dopo*, Giappichelli, 2022, pp. 259-338.

[19]A. Predieri, *Premessa ad uno studio sullo Stato come produttore di informazioni*, in "Studi in onore di Giuseppe Chiarelli", Giuffrè, vol. II, 1974, p. 1615 affermava già da tempo che lo Stato è «un sistema di informazioni e di comunicazioni, e cioè un apparato che raccoglie, immagazzina, elabora e comunica dati».

[20]La centralità delle informazioni in tutti i processi di sviluppo economico e sociale, ricavabili e disponibili con le ICT, hanno reso tutti gli attori sociali – comprese le amministrazioni pubbliche – dei soggetti informativi, cioè dei soggetti che nello svolgimento delle proprie attività possiedono, producono, conservano dati, li processano e li analizzano, producono informazioni e, dunque, nuova conoscenza. I soggetti informativi interagiscono, si relazionano tra di loro con le stesse ICT, ma soprattutto utilizzano questo bagaglio informativo e conoscitivo prodotto dai dati e dalle tecnologie in proprio possesso per perseguire i propri interessi particolari oppure interessi di rilievo pubblico. In questo senso si v. L. Floridi, *La rivoluzione dell'informazione*, Codice Edizioni, 2012.

[21]Sull'emersione di una nuova funzione amministrativa di gestione dei dati e delle informazioni si v. F. Merloni (a cura di), *L'informazione delle pubbliche amministrazioni*, cit. Recentemente anche G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2017.

[22]Sulla centralità del regime dei dati pubblici in questo contesto si v. i contributi presenti in B. Ponti (a cura di), *Il regime dei dati pubblici*, Maggioli, 2008.

[23]Per «base di dati di interesse nazionale», si intende l'«insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni per l'esercizio delle proprie funzioni». Le basi di dati, infatti «costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate». Tra quelle indicate direttamente nell'art. 60, comma 3-*bis* del Codice dell'amministrazione digitale sono ricomprese, ad esempio: l'Anagrafe nazionale della popolazione residente; la Banca dati nazionale dei contratti pubblici; il Repertorio nazionale dei dati territoriali; il Casellario giudiziale; il Registro delle imprese; gli Archivi automatizzati in materia di immigrazione e di asilo; l'Anagrafe nazionale degli assistiti (ANA); l'Anagrafe delle aziende agricole; l'Archivio nazionale dei veicoli e l'anagrafe nazionale degli abilitati alla guida; il Sistema informativo dell'indicatore della situazione economica equivalente (ISEE); l'Anagrafe nazionale dei numeri civici e delle strade urbane (ANNCSU); l'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese.

[24]Le più intense (e prevalenti) esigenze di coordinamento (anche di carattere informativo) nel settore della contabilità e della finanza pubblica comportano, inoltre, la riserva alla competenza statale dei principi di coordinamento della finanza pubblica, nonché – in via esclusiva (a seguito della l. cost. 20 aprile 2012, n. 1) – della materia "armonizzazione dei bilanci pubblici".

[25]B. Ponti, *Coordinamento e governo dei dati nel pluralismo amministrativo*, in "Informatica e diritto", 2008, n. 1-2,

pp. 423-433; M. Falcone, *La cattiva applicazione dei poteri repubblicani nella crisi del disegno regionalista italiano*, in "Diritti regionali. Rivista di diritto delle autonomie territoriali", 2022, n. 1, pp. 360-379.

[26]Si v. l'art. 60, comma 3-*ter* del CAD. L'AgID sulla base di questa disposizione ha individuato attraverso il Piano Triennale per l'Informatica nella PA (2017-2019): il Pubblico registro automobilistico (PRA); l'Anagrafe tributaria; il Catalogo dei dati delle Pubbliche amministrazioni; il Catalogo dei servizi a cittadini e imprese; il Sistema informativo nazionale federato delle infrastrutture (SINFI).

[27]La Piattaforma Nazionale Digitale Dati è stata istituita con il d.lgs. 13 dicembre 2017, n. 217, che ha introdotto l'art. 50-*ter* all'interno del Codice dell'amministrazione digitale. La Piattaforma «è costituita da un'infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici per le finalità di cui al comma 1, mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa, nonché la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite» (art. 50-*ter*, co. 2). Per un approfondimento si v. A. Contaldo, *La piattaforma digitale nazionale dei dati e l'algoritmo: la coesistenza della trasparenza amministrativa con l'efficienza dell'informatizzazione*, in "Lo Stato", 2022, n. 18, pp. 271-284; A. Sandulli, *Pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in "Rivista trimestrale di diritto pubblico", 2021, n. 2, pp. 513-527.

[28]Attualmente i dati contenuti nella Piattaforma sono quelli individuati come basi di dati di interesse nazionale *ex* articolo 60, comma 3-*bis* e le banche dati dell'Agenzia delle entrate individuate dal Direttore della stessa Agenzia. Nella Piattaforma Nazionale Digitale Dati non confluiscono i dati attinenti a ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria. Per accedere a questi dati, le amministrazioni devono accreditarsi alla piattaforma, sviluppare le interfacce di programmazione delle applicazioni (API), attraverso le quali accedere e operare all'interno della Piattaforma, e rendere disponibili le proprie basi dati, in modo tale che tutte le altre amministrazioni possano accedervi facilmente. Una condivisione che deve avvenire nel rispetto delle regole tecniche e infrastrutturali del Sistema pubblico di connettività e cooperazione (*ex* art. 73, comma 1 del CAD), volte a salvaguardare le esigenze di interoperabilità, di coordinamento informativo e di tutela dei dati personali.

[29]In particolare si v. l'art. 50 del CAD. Di particolare importanza è l'introduzione del principio *once only*, secondo il quale le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite loro, ribadito nel Piano triennale per l'informatica nella Pubblica Amministrazione – Aggiornamento 2021-2023.

[30]In questo senso l'art. 53 del CAD, nonché le disposizioni contenute nella l. 9 gennaio 2004, n. 4.

[31]In questo senso si v. la parte ricostruttiva presente in B. Ponti, *La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi*, in "Il Diritto dell'informazione e dell'informatica", 2019, n. 2, pp. 383-422.

[32]Sulle disposizioni attualmente in vigore si v. R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021.

[33]Il d.l. 8 ottobre 2021, n. 139 convertito nella legge 3 dicembre 2021, n. 205, che ha apportato alcune importanti modifiche al d.lgs. 10 agosto 2018, n. 101.

[34]Si veda l'art. 29, comma 4-*bis* del d.lgs. 18 aprile 2016, n. 50, da ultimo modificato dall'art. 53, co. 5, lett. a), sub. 5), della l. 29 luglio 2021, n. 108, che afferma: «L'interscambio dei dati e degli atti tra la Banca Dati Nazionale dei Contratti pubblici dell'ANAC, il sistema di cui al decreto legislativo 29 dicembre 2011, n. 229, e le piattaforme telematiche ad essa interconnesse avviene, nel rispetto del principio di unicità del luogo di pubblicazione e di unicità dell'invio delle informazioni, in conformità alle Linee guida AgID in materia di interoperabilità. L'insieme dei dati e delle informazioni condivisi costituiscono fonte informativa prioritaria in materia di pianificazione e monitoraggio di contratti. Per le opere pubbliche si applica quanto previsto dall'articolo 8, comma 2, del decreto legislativo 29 dicembre 2011, n. 229».

[35]Con potere computazionale non facciamo riferimento alla semplice capacità computazionale abilitata dall'utilizzo delle tecnologie di informazione e di comunicazione, cioè alla capacità/possibilità di elaborare dati e informazioni, ma al vantaggio conoscitivo che questa abilita e al potere di fatto che ne consegue nei rapporti tra soggetti. In questo senso si v. M. Durante, *Il potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Meltemi, 2019.

[36]Sui caratteri dei big data si v. per tutti M.A. Beyer, D. Laney, *The importance of big data: A definition*, Gartner Retrieved, 21 June 2012. Per tutti si v. di V. Mayer-Schönberger, K.N. Cukier, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà* (trad. it. R. Merlini), Garzanti, 2013.

[37]Ancora sulla conoscenza algoritmica si v. A. Gandomi, M. Haider, *Beyond the hype: Big data concepts, methods and analytics*, in "International Journal of Information Management", vol. 35, 2015, pp. 137-144; B. Marr, *Big data: The 5 Vs Everyone Must Know*, 2014. Sulla variabilità si v. E. McNulty, *Understanding Big Data: The seven V's*, in "Dataconomy", 22 May 2014. Sulla capacità di integrazione si v. D. Boyd, K. Crawford, *Critical questions for big data*, in "Information, Communication & Society", vol. 15, 2012, pp. 662-679. Sulla estendibilità e la scalabilità si v. N. Marz, J. Warren, *Big Data: Principles and Best Practices of Scalable Realtime Data Systems*, Manning, 2012.

[38]In questo senso M. Falcone, *"Big data" e pubbliche amministrazioni*, cit. In senso parzialmente diverso si v. F. Costantino, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei "big data"*, in "Diritto pubblico", 2019, n. 1, pp. 43-70.

[39]In questo senso si v. i modi attraverso i quali l'Istat utilizza la c.d. statistica sperimentale. Oppure le attività che la Fondazione Bordoni svolge per l'AGCOM.

[40]Un aspetto che si evince chiaramente consultando il sito della Piattaforma e in cui si fa riferimento alla possibilità di utilizzarla anche per la *data analytics* dei dati in essa contenuti.

[41]Sui casi concreti di utilizzo delle tecnologie algoritmiche nelle amministrazioni si v. A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, cit.; R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data*, cit. Sui rischi derivanti dall'utilizzo delle tecnologie algoritmiche nell'esercizio delle funzioni amministrative, che sono emerse anche dall'azione amministrativa si v. G. Avanzini, *Decisioni amministrative e algoritmi informatici*, cit.; S. Civitarese Matteucci, *Umano troppo umano*, cit.; E. Carloni, *I principi della legalità algoritmica*, cit.; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", 2019, n. 1, pp. 78-79.

[42]In questo senso è andato l'ordinamento europeo con l'art. 22 del GDPR. Per approfondire si v. E. Falletti, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in "Il Diritto dell'informazione e dell'informatica", 2020, n. 2, pp. 169-206; F. Lagioia, G. Sartor, A. Simoncini, *Commento all'art. 22*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy", cit., pp. 378-390.

[43] *Ivi*.

[44] Queste misure sono state esplicitate dal Gruppo di lavoro Articolo 29 (WP29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adottato il 3 ottobre 2017 e revisionato il 3 febbraio 2018.

[45] a) le scelte progettuali pertinenti; b) la raccolta dei dati; c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione; d)la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino; e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; f) un esame atto a valutare le possibili distorsioni; g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

[46] Art. 10, co. 3.

[47] Usa il temine legalità algoritmica E. Carloni, *I principi della legalità algoritmica*, cit. e G. Marchianò, *La legalità algoritmica nella giurisprudenza amministrativa*, in "Il diritto dell'economia", 2020, n. 2, pp. 229-258.

[48] Corsivo mio. Il Consiglio di Stato richiama il regolamento generale sulla protezione dei dati personali in particolare in Cons. Stato, sez.VI, sentt. 8472, 8473, 8474/2019 e nella sent. 881/2020, mentre il testo virgolettato è riferibile a Cons. Stato, Sez. VI, sent. 2270/2019, in cui emerge bene il rilievo organizzativo della decisione algoritmica per garantire la conoscibilità della stessa.

[49] Corsivo mio. Cons. Stato, sez.VI, sentt. 881/2020 e 1206/2021.

* * *

Public authorities information needs and legality: which legal predetermination of public information choices?

Abstract: The essay investigates the close relationship that exists between the principle of legality and the activities of identification and satisfaction of the cognitive needs of the administrations. A relationship that has evolved over time and that today, with the development and progressive use of big data and algorithms in administrative action, needs a new structure.

Keywords: Algorithms – Legality – Databases

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0086
Articolo sottoposto a peer review

La gestione del rischio informatico nella decisione amministrativa robotica

Luigi Previti

Il presente contributo mira ad analizzare uno dei principali rischi connessi all'avanzamento del processo di algoritmizzazione delle decisioni amministrative, ossia quello relativo alla tutela della sicurezza informatica. Nello specifico, dopo aver ricostruito l'articolato sistema multilivello definito negli ultimi anni in materia di cybersicurezza, l'indagine evidenzia la necessità di assicurare un livello adeguato di resilienza cibernetica in sede di automazione delle diverse procedure amministrative, formulando alcune considerazioni finali in merito alla stessa legittimità del ricorso alle formule algoritmiche ai fini decisionali.

Intelligenza artificiale – Decisioni amministrative robotiche – Cybersicurezza – Rischio informatico

Sommario: *1. Decisioni amministrative ai tempi della Società del rischio tecnologico – 2. Le sfide della cibernetica per l'azione amministrativa – 3. La sfida più importante (e spesso dimenticata): pubblico e privato di fronte alle trappole della rete informatica – 4. Verso una pubblica amministrazione "security by design"*

1. Decisioni amministrative ai tempi della Società del rischio tecnologico

Negli ultimi anni dottrina e giurisprudenza sono tornate ad interrogarsi in merito alle sfide, concettuali e operative, poste dall'avanzamento del processo di digitalizzazione dell'azione amministrativa.

Nell'attuale contesto economico e sociale, fortemente condizionato dall'avvento della "Società del rischio" e della "Società Algoritmica", l'uso delle tecnologie informatiche non incide più, infatti, sulle sole modalità di comunicazione tra pubblico e privato o sulle modalità di gestione dei singoli procedimenti, ma si riverbera direttamente sulle modalità con le quali le pubbliche amministrazioni adottano le proprie decisioni e orientano le proprie attività istituzionali nei confronti degli amministrati[1].

In considerazione delle significative opportunità offerte dall'utilizzo delle formule algoritmiche nella cura degli interessi pubblici si è assistito, di conseguenza, a numerosi tentativi di inquadramento teorico e di adeguamento interpretativo del fenomeno, con l'obiettivo di ricondurre anche le tecnologie più sofisticate alle regole e ai principi che connotano l'agire procedimentale dei pubblici poteri[2].

Tuttavia, accanto al crescente interessamento, a livello nazionale ed europeo, per le possibili applicazioni dei sistemi di intelligenza artificiale nel settore pubblico, un analogo interesse non pare essere stato mostrato, se non da ultimo, nei confronti della dimensione organizzativa e, più in particolare, nei confronti delle rilevanti problematiche legate alla salvaguardia della pubblica sicurezza cibernetica (o c.d. cybersicurezza).

Fino ad ora gli ordinamenti giuridici moderni hanno assicurato un livello minimo di sicurezza collettiva attraverso la codificazione di un sistema istituzionale fortemente radicato su categorie e principi chiari e definiti, quali il primato della legge come garanzia dei

L. Previti è ricercatore a tempo determinato di Diritto amministrativo presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Palermo. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

diritti individuali, la spazialità dell'applicazione delle norme giuridiche, il ricorso a meccanismi di prevenzione e di contrasto alla criminalità che si fondano sull'intervento degli apparati delle Forze dell'ordine. Queste coordinate concettuali rischiano, tuttavia, di non essere più adatte ad affrontare le criticità derivanti dalla diffusione della nuova dimensione cibernetica, all'interno della quale vengono rimesse in discussione sia l'applicazione degli istituti giuridici consolidati sia il ruolo tradizionalmente esercitato dai diversi organi politici e burocratici.

Pur mantenendo una prospettiva di indagine assiologicamente neutrale, il presente contributo mira dunque ad evidenziare uno dei principali rischi connessi al repentino sviluppo del processo di robotizzazione delle attività amministrative[3], ossia quello relativo alla tutela della sicurezza cibernetica.

In particolare, dopo aver rimarcato il carattere ontologicamente rischioso di ogni operazione procedurale condotta tramite sistemi informatici, verranno analizzate, seppur brevemente, le caratteristiche e l'articolazione dell'attuale architettura multilivello in materia di cybersicurezza, con l'obiettivo di trarre, a margine di tale indagine, alcune implicazioni sistematiche in ordine alla stessa legittimità del ricorso all'automazione decisionale all'interno del nostro ordinamento.

2. Le sfide della cibernetica per l'azione amministrativa

La progressiva ingegnerizzazione delle funzioni amministrative ha reso non ulteriormente procrastinabile l'esigenza di implementare un sistema istituzionale in grado di individuare e gestire le peculiari incertezze e criticità che tale fenomeno inevitabilmente comporta.

Anche le riflessioni dottrinali che da ultimo si sono occupate di indagare l'ammissibilità e le modalità di utilizzo dei diversi sistemi di intelligenza artificiale all'interno del settore pubblico sembrano ormai concordare sull'impossibilità di sfruttare a pieno i vantaggi derivanti dalla crescente informatizzazione dell'azione amministrativa prescindendo dall'analisi del grado e della tipologia dei rischi riconducibili alle nuove tecnologie[4].

Uno dei rischi più evidenti in materia è certamente quello relativo all'opacità dell'*iter* decisionale seguito dalle pubbliche amministrazioni[5].

Com'è noto, infatti, le moderne tecnologie non possono essere assimilate a quelle in uso nei primi anni degli anni '90, dal momento che queste non si limitano più ad attuare pedissequamente le specifiche istruzioni elaborate dal programmatore, ma sono dotate della capacità di definire, a loro volta, percorsi decisionali talora non prevedibili e non verificabili *a posteriori*.

Sicché, se neppure colui che ha fornito le istruzioni è pienamente in grado di ripercorrere il procedimento logico-matematico seguito dal software e offrire una ragionevole spiegazione della decisione adottata, la preoccupazione maggiormente avvertita è quella di costruire un modello di pubblica amministrazione che si caratterizza per essere, da un lato, più moderna ed efficiente, ma, dall'altro, più oscura e imperscrutabile.

Una circostanza in grado di riflettersi, a ben vedere, anche sullo stesso ruolo del funzionario amministrativo chiamato ad adottare il provvedimento finale, il quale potrebbe assumere, nel nuovo contesto digitalizzato, una funzione più formale e rappresentativa rispetto al passato, laddove il ruolo di decisore sostanziale (seppur "invisibile") verrebbe sostanzialmente affidato all'elaboratore elettronico.

Accanto al rischio di opacità o di invisibilità dell'amministrazione algoritmica, la dottrina ha più volte evidenziato il rischio di pervenire ad esiti discriminatori[6].

Ogni processo di automazione richiede, in primo luogo, l'esecuzione di un'operazione di traduzione delle istruzioni redatte in linguaggio umano (ossia, i criteri di valutazione, i riferimenti normativi, i passaggi logici, ecc.) in un linguaggio tecnico, comprensibile per la macchina.

Tale operazione non costituisce, tuttavia, un'attività di natura meccanica, ma rappresenta, invece, un momento procedurale estremamente delicato, nel quale è ben possibile che si verifichino traduzioni semantiche infedeli, imprecise o errate, in grado di condurre all'adozione di decisioni finali irragionevoli e/o discriminatorie.

Allo stesso tempo, è ben possibile che la violazione del principio di non discriminazione si realizzi per la scarsa qualità dei dati acquisiti dal software. Una circostanza che conduce a riflettere sulla necessità di garantire, quantomeno in alcuni casi, appositi momenti di controllo degli esiti procedurali raggiunti dalla macchina, al fine di verificare che le regole di funzionamento della procedura automatizzata definite *ex ante* siano rispettate prima dell'adozione del provvedimento amministrativo.

A ciò si aggiunga che il rischio di ottenere una decisione amministrativa contraria al principio di non discriminazione è molto più elevato qualora vengano adoperati algoritmi di tipo non deterministico. È in queste ipotesi, infatti, che è necessario richiedere all'amministrazione procedente di svolgere un controllo più penetrante e costante, dal momento che, in tali fattispecie, non è sempre possibile garantire che il risultato della procedura automatizzata sia in linea con le finalità e i criteri di giudizio definiti in sede di progettazione.

Più di recente, il tema della gestione del rischio legato all'utilizzo di sistemi e procedure informatizzate è stato oggetto di specifica attenzione a livello sovranazionale, come si evince dalla recente proposta di regolamento europeo sull'intelligenza artificiale, pubblicata dalla Commissione europea il 21 aprile 2021[7].

Con tale atto è stata suggerita, per la prima volta, l'introduzione di un quadro omogeneo di condizioni e di requisiti minimi ispirati ad una logica di tipo *risk-based*, ossia parametrati allo specifico livello di rischio che i singoli sistemi informatici presentano nei confronti della sicurezza, della salute e della sfera giuridica individuale. Un approccio metodologico che si fonda, in particolare, sulla fissazione di limitazioni d'uso e di obblighi di progettazione chiari e proporzionati, sul contenimento dei costi di conformità alla normativa di settore da parte degli operatori economici e sulla previsione di oneri di monitoraggio e di segnalazione degli incidenti in capo agli stessi utenti.

Se è dunque chiaro che un uso irragionevole e indisciplinato della tecnologia può rappresentare un grave e serio rischio per i diritti e le libertà fondamentali, diviene sempre più pressante l'esigenza di monitorare e salvaguardare il livello di sicurezza cibernetica raggiunto a livello nazionale, quale strumento centrale per prevenire e contrastare il diffondersi di indebite intrusioni, manomissioni e alterazioni ad opera dei sempre più pericolosi criminali informatici.

3. La sfida più importante (e spesso dimenticata): pubblico e privato di fronte alle trappole della rete informatica

L'obiettivo di tutelare la sicurezza delle reti e dei dispositivi elettronici viene espressamente menzionato negli atti di indirizzo di livello europeo quantomeno a partire dai primi anni del XXI secolo, ove si rimarca la circostanza secondo la quale la cybersicurezza rappresenta la naturale precondizione per la crescita e lo sviluppo sostenibile degli Stati tecnologicamente avanzati[8].

Tuttavia, la necessità di assicurare un livello più elevato di protezione dei diritti degli operatori pubblici e privati che utilizzano, per diverse finalità, le moderne tecnologie ha condotto solo negli ultimi anni le istituzioni dell'Unione ad adottare un quadro normativo maggiormente chiaro e definito.

Sotto questa prospettiva, l'interesse del legislatore per la predisposizione di un apparato pubblicistico di contrasto nei confronti delle minacce cibernetiche rappresenta il necessario contraltare rispetto all'impulso verso lo sviluppo e la diffusione di applicazioni informatiche sempre più sofisticate e interconnesse[9].

Al riguardo occorre osservare come la definizione di una solida ed efficace strategia in materia di cybersicurezza sia strettamente correlata alle politiche europee di implementazione del mercato unico digitale, all'interno del quale si intende garantire non solo un'ampia offerta di servizi digitali personalizzati, ma anche un soddisfacente grado di resilienza contro il rischio di attacchi cibernetici[10].

Il raggiungimento di tale finalità ispira chiaramente la direttiva UE 2016/1148, nota anche come "direttiva NIS" (*Network and Information Security*), che rappresenta il primo importante tentativo di armonizzazione delle legislazioni nazionali in tema di sicurezza informatica[11].

Nello specifico, la direttiva ha stabilito una serie di rilevanti misure tecniche ed organizzative per due determinate categorie di soggetti, ossia i c.d. "operatori dei servizi essenziali" (OSE) e i "fornitori di servizi digitali" (FSD), la cui intensità è direttamente proporzionale alla strategicità e alle dimensioni dei singoli destinatari[12].

Si tratta di obblighi principalmente rivolti a rendere più affidabili le reti utilizzate dai predetti soggetti, a prevedere e minimizzare l'impatto delle minacce più significative sulla continuità delle operazioni e dei servizi svolti, nonché ad assicurare la tempestiva comunicazione degli incidenti di sicurezza alle competenti autorità nazionali NIS.

Più di recente, il legislatore europeo è intervenuto per rivedere e aggiornare le linee strategiche e operative precedentemente stabilite[13]. Una decisione sulla quale hanno certamente influito sia la consapevolezza dell'intensificarsi e dell'evoluzione delle minacce cibernetiche a livello globale[14], sia l'intenzione di affermare una più chiara visione europea del cyberspazio[15].

In questo senso vanno lette le disposizioni introdotte dal regolamento UE 2019/881, c.d. *Cybersecurity Act*[16], il quale si caratterizza per la previsione di due significativi interventi: il primo riguarda l'istituzione di un sistema europeo di certificazione della cybersicurezza, ossia un insieme di regole e procedure volte ad assicurare, all'interno del territorio dell'Unione, la conformità di prodotti, servizi e processi ICT rispetto a determinati parametri minimi di sicurezza informatica; il secondo riguarda il rafforzamento dei poteri istituzionali dell'Agenzia europea per la cybersicurezza (*European Union Agency for Network and Information Security*, di seguito ENISA), autorità istituita nel 2004 con lo scopo di assistere le istituzioni europee e gli Stati membri nello sviluppo e nella revisione delle politiche e delle azioni strategiche in materia.

Nell'ambito del nuovo mandato, viene così attribuito all'Agenzia il compito di fornire pareri, consulenze e orientamenti, sostenere lo scambio di informazioni e di buone pratiche, promuovere il miglioramento delle tecniche di prevenzione, analisi e reazione nei confronti delle minacce più pericolose, stimolare l'aggiornamento della normativa europea di settore, supportare la rete europea dei CSIRT, incentivare l'uso del citato meccanismo di certificazione dei prodotti e dei servizi ICT e sensibilizzare l'opinione pubblica sui rischi informatici attualmente più diffusi. Si tratta, a ben vedere, di iniziative che perseguono chiari obiettivi di cooperazione interistituzionale, di coordinamento operativo e di incremento qualitativo delle misure organizzative, nonché di risposta alle situazioni di crisi di portata transfrontaliera aventi ad oggetto settori nevralgici dell'economia[17].

Volgendo lo sguardo al livello nazionale, è possibile osservare come la costruzione di un apposito sistema istituzionale di gestione dei rischi derivanti dal crescente aumento delle minacce informatiche sia stata affidata, in un primo momento, a fonti normative di rango non primario, attraverso le quali si è realizzato il coordinamento di corpi amministrativi preesistenti, principalmente attivi nel «Sistema di informazione per la sicurezza della Repubblica» di cui alla l. 3 agosto 2007, n. 124.

All'interno di tale contesto, un ruolo di cruciale importanza viene affidato al Presidente del Consiglio dei ministri, nella qualità di vertice del citato Sistema di informazione per la sicurezza, al quale è attribuita la definizione degli indirizzi e degli obiettivi generali della politica di sicurezza cibernetica. Tale funzione trova concreta manifestazione, segnatamente, nell'elaborazione di direttive[18] e di documenti programmatici, come il Quadro strategico nazionale e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, che mirano a rafforzare la protezione delle infrastrutture critiche, materiali e immateriali, presenti sul territorio[19].

L'attuazione degli indirizzi e degli obiettivi fissati nei suddetti atti viene devoluta, invece, a una pluralità di organismi di supporto e di coordinamento operativo, tra i quali occupano una posizione di rilievo: il Comitato interministeriale per la sicurezza della Repubblica - CISR, con funzioni di consulenza rispetto agli atti di indirizzo di competenza del Presidente del Consiglio e di proposta rispetto alle misure normative e organizzative ritenute necessarie[20]; il Dipartimento delle informazioni per la sicurezza della Repubblica (di seguito, DIS), incaricato di presiedere tutte le attività di ricerca, di analisi e di elaborazione informativa relative alle minacce e agli attacchi cibernetici[21]; il Nucleo per la Sicurezza Cibernetica, istituito dal d.P.C.M. n. 66/2013 al fine di coordinare l'azione di tutti i soggetti coinvolti nella preparazione e nella gestione delle situazioni di crisi e di attivare le eventuali procedure di allerta e di risposta[22].

Seppur improntato ad un principio di razionale distribuzione delle funzioni tra i diversi attori istituzionali, il disegno normativo sopra descritto, tuttavia, si è rivelato presto alquanto complesso e inefficiente.

A tali lacune cercano di porre rimedio il successivo d.P.C.M. 17 febbraio 2017[23], nonché, in aderenza alle sollecitazioni europee, il d.lgs. 18 maggio 2018, n. 65, che recepisce la ricordata direttiva NIS, il d.l. 21 settembre 2019, n. 105, convertito dalla l. 18 novembre 2019, n. 133, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica - PSNC[24] e il d.l. 14 giugno 2021, n. 82, convertito dalla l. 4 agosto 2021, n. 109, che ha istituito, con colpevole ritardo rispetto alle esperienze di altri Paesi, l'Agenzia per la cybersicurezza nazionale.

Alla predetta autorità il d.l. n. 82/2021 ha affidato compiti e responsabilità peculiari, che riguardano, principalmente, la prevenzione e la tutela della sicurezza nazionale nel cyberspazio, l'ispezione, l'accertamento e l'irrogazione delle sanzioni prescritte in caso di violazione della normativa di settore, la gestione delle vulnerabilità informatiche e le attività di contrasto in caso di attacco[25].

Nell'ambito di queste ultime attività, funzioni di grande rilevanza sono attribuite al CSIRT Italia, introdotto in sede di recepimento della direttiva NIS e incardinato, dapprima, presso il DIS e, oggi, trasferito presso l'Agenzia[26]. Spetta al predetto gruppo di intervento, in particolare, monitorare periodicamente il verificarsi di attacchi e di incidenti a livello nazionale, ricevere le segnalazioni obbligatorie provenienti dagli OSE e dai FSD di cui alla direttiva NIS e le segnalazioni facoltative provenienti dagli altri soggetti, pubblici e privati, comunque interessati da una minaccia *cyber*, emettere preallarmi e allerte e offrire assistenza operativa in situazioni di crisi.

All'Agenzia nazionale spettano, inoltre, importanti compiti di promozione e di coordinamento delle iniziative e dei progetti rivolti alla formazione e alla sensibilizzazione collettiva sulle problematiche riguardanti la cybersicurezza. Attività che vengono espletate sia tramite il supporto di un organo interno, ossia il Comitato tecnico-scientifico, sia tramite il coinvolgimento delle università, degli enti di ricerca, del sistema produttivo nazionale e delle altre istituzioni pubbliche competenti.

L'istituzione dell'autorità, che opera quale interlocutore unico per i soggetti ricompresi nel PSNC, pare conferire maggiore compattezza ad un disegno normativo inizialmente frammentato e complesso, che

risulta oggi improntato all'accentramento delle competenze e al coordinamento delle linee strategiche e delle azioni operative, nell'ottica della semplificazione delle procedure decisionali e dell'eliminazione delle preesistenti sovrapposizioni funzionali[27].

Le suddette scelte di governance, per quanto aderenti alle indicazioni di matrice europea, paiono riflettere, invero, l'intenzione del legislatore nazionale di salvaguardare le sole infrastrutture strategiche per la vita economica e sociale del Paese, laddove sarebbe stato più opportuno estendere la copertura assicurata dall'architettura istituzionale nei confronti di soggetti ed enti di rilevanza nazionale, sebbene non rientranti nel menzionato PSNC.

4. Verso una pubblica amministrazione "security by design"

L'analisi del sistema multilivello congegnato in materia di cybersicurezza consente di svolgere alcune considerazioni finali in merito alle attuali esigenze di prevenzione e di contrasto nei confronti dei sempre più frequenti attacchi informatici all'interno del settore pubblico.

A tal proposito alcune interessanti indicazioni parrebbero potersi trarre dai recenti principi affermati *in subiecta materia* a livello sovranazionale[28].

Da un lato, assume rilevanza il c.d. principio di "sicurezza *by design*", in base al quale i produttori e i fornitori devono immettere sul mercato unicamente beni e/o servizi in grado di assicurare determinati livelli di resilienza contro il rischio di incidenti e attacchi. Un'obbligazione, quest'ultima, che non solo deve essere rispettata fin dal momento della progettazione dell'infrastruttura o del dispositivo, ma che costituisce altresì una specifica parte della prestazione contrattuale assunta dal professionista nei confronti del consumatore[29].

Dall'altro, merita di essere richiamato il c.d. "principio di responsabilità", in virtù del quale gli operatori economici del settore devono assumere, nei confronti degli utenti della rete, il ruolo di interlocutori privilegiati durante l'intero ciclo di vita dei prodotti ICT acquistati sul mercato. Una circostanza che determina per tali soggetti il sorgere di un particolare dovere di diligenza, che si esplica, ad esempio, nell'obbligo di curare i necessari aggiornamenti software dei prodotti, di risolvere con celerità le vulnerabilità segnalate dai consumatori, nonché di garantire un corretto utilizzo dei dati personali trattati nello svolgimento delle proprie attività imprenditoriali[30].

In altri termini, secondo la moderna visione europea di cyberspazio, tutte le imprese che intendono offrire i propri prodotti online hanno l'obbligo di mantenere e preservare un soddisfacente livello di sicurezza delle reti e dei sistemi informatici utilizzati, assumendosi la responsabilità di ogni eventuale danno o pregiudizio cagionato a terzi in ragione dell'inadempimento della suddetta obbligazione.

Declinando le suddette indicazioni all'interno dello specifico contesto dell'automazione delle procedure amministrative, non parrebbe irragionevole pretendere, oltre a quelle garanzie procedimentali fissate dall'ormai nota giurisprudenza amministrativa[31], anche il rigoroso rispetto, fin dalla progettazione (*by design*), di un adeguato livello di *cyber*-resilienza per le piattaforme, i dispositivi e i dati utilizzati dalla pubblica amministrazione.

Seguendo tale ragionamento, in particolare, sarebbe possibile giungere ad elevare la sicurezza dei software e delle reti informatiche coinvolti nei processi di automazione in un ulteriore requisito minimo di legittimità delle decisioni amministrative robotiche, la cui mancanza ben potrebbe essere censurata in sede giurisdizionale, con tutte le conseguenze sul piano risarcitorio che da ciò potrebbero discendere.

Si auspica, pertanto, una futura adesione giurisprudenziale ad una siffatta impostazione, la quale pare poter concorrere effettivamente all'accrescimento del senso di fiducia dei cittadini nei confronti dell'intelligenza artificiale e delle sue applicazioni, nonché alla realizzazione di una visione autenticamente antropocentrica del processo di algoritmizzazione delle procedure amministrative.

Note

[1]Sul concetto di "Società dell'Algoritmo", è doveroso il rinvio a J.M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in "Ohio State Law Journal", 2017, n. 78, p. 1219, secondo il quale la predetta locuzione identificherebbe «a society organized around social and economic decision-making by algorithms, robots, and AI agents, who not only make the decisions but also, in some cases, carry them out». Sui rischi connessi alla diffusione del c.d. "ignoto tecnologico", si veda, invece, il lavoro di A. Barone, *Il diritto del rischio*, Giuffrè, 2006, *passim*. Più in generale, sulla possibilità di qualificare la società contemporanea come "Società del rischio", si vedano, per tutti, U. Beck, *La società del rischio. Verso una seconda modernità*, Carocci, 2000, spec. p. 25 ss., ove l'A. sottolinea che «nella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale di rischi» e, in particolare, quelli «prodotti dalla scienza e dalla tecnica», nonché F. Fukuyama, *L'uomo oltre l'uomo. Le conseguenze della rivoluzione biotecnologica*, Mondadori, 2002.

[2]Per una ricostruzione analitica delle diverse posizioni dottrinali e giurisprudenziali affermatesi nel tempo *in subiecta materia* sia consentito rinviare a L. Previti, *La decisione amministrativa robotica*, Editoriale Scientifica, 2022.

[3]Come ricorda A. Santosuosso, *Diritto, scienza, nuove tecnologie*, Cedam, 2016, p. 323, il termine "robot", di origine ceca, significa letteralmente "lavoro duro/pesante" ed è stato coniato, per la prima volta, dal drammaturgo Karel Capek,

negli anni '20 del XX secolo, per riferirsi ad umanoidi adibiti al lavoro di schiavi, creati dall'uomo con il precipuo scopo di sollevarlo dalla fatica fisica. Con l'espressione "decisione amministrativa robotica" ci si riferisce, dunque, a quelle decisioni assunte dalle pubbliche amministrazioni attraverso il ricorso ad appositi sistemi informatici, ossia a quell'istituto che parte della dottrina etichetta talora con le espressioni "decisione amministrativa automatizzata" e "decisione amministrativa algoritmica" (locuzioni, quest'ultime, invero alquanto generiche, in considerazione della diversità, oltre che dei livelli di automazione decisionale, delle tipologie di formule algoritmiche attualmente esistenti).

[4]In materia, cfr. ancora A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in "European Review of Digital Administration Law", 2020, n. 1-2, p. 65 ss., secondo il quale l'intera tematica dell'IA è dominata dalle esigenze di regolazione e di gestione dei rischi (sociali, economici, tecnici) che possono derivare dall'uso delle nuove tecnologie.

[5]In materia, cfr. J. Barrat, *Our Final Invention: Artificial intelligence and the End of the Human Era*, Thomas Dunne Books, 2013; F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015; C. Coglianese, D. Lehr, *Regulating by Robot. Administrative Decision Making in the Machine-Learning Era*, in "Georgetown Law Journal", 2017, n. 105, *passim*; B.D. Mittelstadt, P. Allo, L. Floridi et al., *The ethics of algorithms. Mapping the debate*, in "Big data & Society", 2016, n. 21, p. 3 ss.; A. Cerrillo i Martínez, *How can we open the black box of public administration? Transparency and accountability in the use of algorithms*, in "Revista Catalana de Dret Públic", 2019, n. 58, p. 15 ss.

[6]Sui rischi di discriminazione riconducibili all'utilizzo di meccanismi decisionali robotici, si vedano, *ex multis*, F. Costantino, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in "Diritto pubblico", 2019, n. 1, p. 56 ss.; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", 2019, n. 1, p. 84 ss.; F. De Leonardis, *Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, in E. Calzolaio (a cura di), "La decisione nel prisma dell'intelligenza artificiale", Cedam, 2020, p. 152 ss.; M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in "federalismi.it", 2019, n. 16, p. 19; G. Pesce, *Il Consiglio di Stato ed il vizio dell'opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in "www.giustizia-amministrativa.it", 16 gennaio 2020, p. 12 ss.; P. Savona, *Administrative Decision-Making after the Big Data Revolution*, in "federalismi.it", 2018, n. 19, p. 22 ss.

[7]Cfr. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, COM(2021) 206 final. In materia si vedano, quantomeno, G. Marchianò, *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, in "Ambientediritto.it", 2021, n. 2; C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in "BioLaw Journal", 2021, n. 3, p. 415 ss.; G. De Gregorio, F. Paolucci, O. Pollicino, *L'intelligenza artificiale made in UE è davvero "umano-centrica"? I conflitti della proposta*, in "Agendadigitale.eu", 22 luglio 2021; F. Lamberti, *La proposta di regolamento UE sull'Intelligenza artificiale alla prova della privacy*, in "federalismi.it", 29 giugno 2022.

[8]Tra i primi interventi normativi in materia si vedano: la comunicazione della Commissione europea del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001) 298, par. 2.1, in base alla quale: «La sicurezza delle reti e dell'informazione va intesa come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema»; la direttiva 2002/21/CE del 7 marzo 2022, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica e affida alle autorità nazionali di regolazione il compito di garantire il mantenimento dell'integrità e della sicurezza delle reti e delle comunicazioni pubbliche (art. 8, co. 4, lett. f); la comunicazione della Commissione europea del 26 settembre 2003, *Il ruolo dell'e-Government per il futuro dell'Europa*, COM(2003) 567, par. 2.1, ove si riconosce che: «In futuro i cittadini esigeranno sempre più che le pubbliche autorità provvedano a tutelare la libertà, la giustizia e la sicurezza in tutta l'Unione europea. Occorre a tal fine garantire una cooperazione tra gli Stati membri e a livello internazionale e fare anche fronte a nuove forme di insicurezza generate dall'utilizzo di nuove tecnologie».

[9]Com'è noto, si assiste oggi ad una moltiplicazione di sistemi e dispositivi costantemente connessi ad internet, in grado di interagire tra di loro e con il mondo fisico attraverso l'uso di appositi sensori, plasmando in tal modo una rete di strumenti informatici ormai nota con l'espressione *Internet of Things* - IoT. Sul punto, cfr. R.H. Weber, E. Studer, *Cybersecurity and the Internet of Things: Legal Aspect*, in "Computer Law & Security Review", 2016, n. 36, p. 726 ss.; A. Rayes, S. Salam, *Internet of Things: from Hype to Reality*, Springer, 2019; L. De Nardis, *The Internet in Everything. Freedom and Security in a World with No Off Switch*, Yale University Press, 2020; G. Noto La Diega, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, 2022.

[10]Comunicazione della Commissione europea del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final. Sul punto, cfr. anche il regolamento UE 2021/694 del 29 aprile 2021 che istituisce il Programma "Europa digitale" (2021-2027): «La fiducia costituisce una condizione essenziale per il funzionamento del mercato unico digitale. Le tecnologie della cybersicurezza, come le identità digitali, la crittografia e il rilevamento delle intrusioni, e le loro applicazioni in ambiti quali il settore finanziario, l'industria 4.0, l'energia, i trasporti, la sanità e l'amministrazione elettronica sono essenziali per salvaguardare la sicurezza e la fiducia nelle attività e nelle operazioni online da parte dei cittadini, delle pubbliche amministrazioni e delle imprese» (considerando 39).

[11]Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016.

[12]In particolare, ai sensi della direttiva NIS gli «operatori dei settori essenziali» sono coloro che svolgono la propria attività economica nel settore della fornitura e distribuzione dell'acqua potabile, dell'energia, dei trasporti, della salute, delle infrastrutture digitali, dei servizi bancari e finanziari; al contrario, sono definiti come «fornitori di servizi digitali» coloro che operano nel settore dei motori di ricerca, dei servizi di cloud computing e delle piattaforme di commercio elettronico. L'applicazione del citato principio di proporzionalità – *rectius*, gradualità – impone che gli obblighi di sicurezza previsti per i primi siano più severi rispetto a quelli previsti per i secondi, atteso il più alto livello di rischio per la stabilità nazionale in caso di attacchi informatici nei confronti degli OSE. In merito al campo di applicazione della direttiva, occorre segnalare le rilevanti modifiche formulate sul punto nella proposta di revisione del 16 dicembre 2020, COM(2020) 823 final (c.d. "direttiva NIS 2"), con la quale la Commissione europea ha manifestato l'intenzione di chiarire ed estendere la portata del precedente atto sia dal punto di vista soggettivo, ossia con riferimento

all'individuazione dei soggetti coinvolti nella catena di gestione del rischio cibernetico (introducendo al riguardo una nuova classificazione dei destinatari degli obblighi di sicurezza, che si divideranno in "essenziali" e "importanti"), sia dal punto di vista oggettivo, ossia con riferimento alla razionalizzazione degli obblighi di comunicazione e degli standard minimi di sicurezza.

[13]La necessità di promuovere una nuova strategia europea in materia di cybersicurezza viene ben rimarcata: nella comunicazione della Commissione e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 final, ove si riconosce, per la prima volta, che: «sempre più spesso gli attori statali raggiungono i loro obiettivi geopolitici non solo attraverso strumenti tradizionali come la forza militare, ma anche attraverso strumenti cibernetici più discreti, volti anche ad interferire nei processi democratici interni» (p. 2); nella comunicazione della Commissione del 19 febbraio 2020, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, ove si precisa che: «Una vera trasformazione digitale deve iniziare dalla fiducia di cittadini e imprese europei nella sicurezza di prodotti e applicazioni. Quanto più siamo interconnessi, tanto più siamo vulnerabili alle attività informatiche dolose»; nella comunicazione della Commissione del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, COM(2020) 605 final, ove si sottolinea che: «L'avvento dell'Internet degli oggetti e il maggiore ricorso all'intelligenza artificiale comporteranno nuovi benefici ma anche una serie di nuovi rischi. [...] La dipendenza da sistemi online ha dato il via a un'ondata di attacchi da parte della cibercriminalità. Il cosiddetto "cybercrime as-a-service" (ossia l'offerta di servizi illegali) e l'economia "cibercriminale" sotterranea offrono un agevole accesso a prodotti e servizi informatici online offerti dalla criminalità informatica» (pp. 3-4); nella comunicazione della Commissione e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN(2020) 18 final, che aggiorna la precedente strategia del 2017.

[14]Si tratta di un fenomeno che ha acquisito un'importanza sempre crescente nell'agenda politica nazionale e dell'Unione a causa dell'accelerazione del processo di digitalizzazione riconducibile all'esperienza della pandemia da COVID-19 e del costante aumento degli episodi di attacchi cibernetici, legati da ultimo anche allo scoppio del drammatico conflitto tra Russia e Ucraina.

[15]In tal senso, si vedano le considerazione espresse nella Risoluzione del Parlamento europeo del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione di quest'ultima per ridurre tali minacce, 2019/2575(RSP), ove si è chiarito come: «l'Unione debba assumere un ruolo guida in materia di cibersicurezza, adottando un approccio comune basato su un utilizzo efficiente ed efficace delle competenze dell'Unione, degli Stati membri e dell'industria, dato che un mosaico di decisioni nazionali divergenti nuocerebbe al mercato unico digitale [...]», e si «invita la Commissione a sviluppare una strategia che ponga l'Europa all'avanguardia nel settore delle tecnologie di cibersicurezza, onde ridurre la dipendenza dell'Europa dalla tecnologia straniera in tale campo».

[16]Regolamento UE 2019/881 del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, che ha abrogato il precedente regolamento UE 526/2013 del 21 maggio 2013.

[17]Sul nuovo ruolo dell'Agenzia, cfr. A. Contaldo, D. Mula (a cura di), *Cybersecurity Law*, Pacini, 2020, p. 71 ss. In tema di cooperazione interistituzionale, occorre richiamare il regolamento UE 2021/887 del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza con l'obiettivo di colmare, nel contesto della rete dei Centri nazionali di coordinamento, il profondo divario di capacità e di competenze esistente nel territorio dell'Unione e di diffondere il più possibile i risultati delle ricerche e delle attività finanziate.

[18]Oltre che nei confronti del Dipartimento delle informazioni per la sicurezza (sul quale *infra*), il potere di direttiva del Presidente del Consiglio dei ministri è esercitato anche nei confronti dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI), le quali svolgono le rispettive attività di ricerca informativa sotto il coordinamento operativo del suddetto Dipartimento (art. 4, co. 3, lett. d-*bis*), l. 3 agosto 2007, n. 124).

[19]In particolare, ai sensi dell'art. 3, co. 1, lett. a) e b), d.P.C.M. 24 gennaio 2013, il Quadro strategico nazionale doveva contenere l'indicazione dei caratteri e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, interessati alla gestione dei sistemi e delle reti di interesse strategico, l'individuazione di strumenti e di procedure tramite i quali migliorare le capacità nazionali di prevenzione e risposta rispetto alle minacce del cyberspazio; il Piano nazionale per la protezione cibernetica doveva indicare, invece, gli obiettivi e le linee di azione da porre in essere per realizzare il predetto Quadro strategico.

[20]Art. 4, co. 1, d.P.C.M. 24 gennaio 2013. Il Comitato è presieduto dal Presidente del Consiglio ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico (art. 5, co. 3, l. 3 agosto 2007, n. 124).

[21]Cfr. art. 4, co. 3, lett. d-*bis*), l. n. 124/2007, introdotto dalla l. 7 agosto 2012, n. 133, e art. 7 d.P.C.M. 24 gennaio 2013 ai sensi del quale il DIS è chiamato, altresì, a trasmettere le informazioni e i dati rilevanti acquisiti al Nucleo per la sicurezza cibernetica, alle pubbliche amministrazioni e agli altri soggetti, pubblici e privati, interessati a ricevere tali informazioni.

[22]Artt. 8 e 9 d.P.C.M. 24 gennaio 2013.

[23]In particolare, il decreto ha rivisto le attribuzioni del Presidente del Consiglio dei ministri, del CISR e del Nucleo per la sicurezza cibernetica nelle situazioni di crisi informatica che coinvolgono aspetti di sicurezza nazionale, al fine di assicurare una risposta maggiormente unitaria e coordinata nella gestione e nella risoluzione delle predette ipotesi. Sulle novità introdotte dal d.P.C.M., si rinvia a L.V.M. Salamone, *La disciplina del* cyberspace *alla luce della direttiva europea delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'*intelligence *e prospettive* de iure condendo, in "federalismi.it", 2017, n. 23, p. 29 ss.

[24]Com'è noto, l'istituzione del Perimetro nazionale risponde all'esigenza di assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti (pubbliche amministrazioni, enti pubblici e privati) che esercitano «una funzione essenziale dello Stato» o che prestano «un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato», seppur non rientranti nell'ambito di applicazione della citata direttiva NIS. Si tratta di soggetti individuati in un apposito elenco, adottato con d.P.C.M., su proposta del Comitato interministeriale per la cybersicurezza, non soggetto a pubblicazione o a istanze di accesso; sicché solo le amministrazioni e gli enti rientranti all'interno del suddetto Perimetro ricevono comunicazione dell'iscrizione (art. 1, co. 2-*bis*, d.l. 21 settembre 2019, n. 105).

[25]Accanto alla menzionata Agenzia, il d.l. n. 82/2021 ha istituito, presso la Presidenza del Consiglio dei ministri, il Comitato Interministeriale per la cybersicurezza (CIC), chiamato a svolgere funzioni consultive, di proposta e di vigilanza in materia di politiche di cybersicurezza del tutto assimilabili

a quelle in precedenza spettanti al CISR (il quale, nel nuovo assetto organizzativo, mantiene un ruolo importante nella gestione delle crisi cibernetiche, ai sensi degli artt. 4, co. 6, e 10 d.l. n. 82/2021).

[26]Le attività del CSIRT Italia sono definite dal d.P.C.M. dell'8 agosto 2019.

[27]In materia, va ricordato che la suddetta Agenzia: predispone la strategia nazionale di cybersicurezza (art. 7, co. 1, lett. b); è qualificata come «Autorità nazionale di certificazione della cybersicurezza» ai sensi dell'art. 58 del citato reg. UE 2019/881, con il compito di coordinare e di dirigere il sistema italiano di certificazione, qualificazione e valutazione della cybersicurezza dei prodotti, servizi e processi ICT (art. 7, co. 1, lett. e), come confermato, da ultimo, dal d.lgs. 3 agosto 2022, n. 123); è designata quale «Centro nazionale di coordinamento» ai sensi dell'art. 6 del citato reg. UE 2021/887, con il compito di supportare il Centro europeo di competenza per la cybersicurezza nell'attività di rafforzamento delle capacità, delle conoscenze e della competitività dell'Unione nel settore (art. 7, co. 1, lett. aa). Per un quadro riassuntivo delle funzioni della nuova Agenzia, si veda S. Aterno, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, 2022, p. 234 ss.

[28]Sul punto, si vedano la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, cit., p. 6, ove si riconosce che: «Un approccio di "sicurezza fin dalla progettazione" adottato dai produttori di dispositivi connessi, software e attrezzature informatiche permetterebbe di definire la questione della cibersicurezza prima di immettere nuovi prodotti sul mercato. Questo potrebbe rientrare nel principio di "responsabilità", da elaborare ulteriormente insieme agli operatori del settore, che potrebbe ridurre le vulnerabilità dei prodotti/software applicando una serie di metodi che vanno dalla progettazione ai test e alla verifica, inclusa la verifica formale ove applicabile, la manutenzione a lungo termine e l'utilizzo di processi sicuri lungo il ciclo di sviluppo, così come lo sviluppo di aggiornamenti e correzioni atti a risolvere vulnerabilità precedentemente nascoste e rapidi interventi di aggiornamento e riparazione»; nonché la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, cit., par. 1.5., ove si precisa che il dovere di diligenza esigibile nei confronti dei produttori dovrà essere potenziato a livello normativo, proprio a causa della crescente diffusione del fenomeno dell'*Internet of things* di cui si è detto *supra*.

[29]Si tratta, invero, di un'obbligazione di non semplice esecuzione, dal momento che, come nota P.L. Montessoro, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in "Istituzioni del federalismo", 2019, n. 3, p. 790, oggi gli hacker investono ingenti risorse nella ricerca degli errori di programmazione (bug), al fine di modificare ad arte il comportamento del calcolatore in cui è inserito il programma difettoso. Sicché «il progettista deve correggere tutte le vulnerabilità del suo sistema, mentre all'hacker basta scoprirne una [...]».

[30]Sui possibili conflitti tra tutela della cybersicurezza e tutela della privacy, si è espresso in più occasioni lo stesso Garante europeo per la protezione dei dati, secondo il quale le recenti iniziative legislative in tema di *cybersecurity* non dovrebbero pregiudicare quanto già previsto dal GDPR, ma dovrebbero, al contrario, ispirarsi ai principi di quest'ultimo, come quelli del *privacy by design* e del *privacy by default* (art. 25 GDPR). Così, European Data Protection Supervisor, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*, 11 marzo 2021; nonché Id., *Opinion 8/2022 on the Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union*, 17 maggio 2022.

[31]Come affermato, da ultimo, da Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472; Id., sez. VI, 4 febbraio 2020, n. 881.

* * *

The cyber risk management in the algorithmic administrative decisions

Abstract: This contribution aims to highlight one of the main risks linked to the progress of the algorithmization of administrative decisions, that is the protection of cybersecurity. In particular, after having analyzed the complex multi-level system defined in recent years in the field of cybersecurity, the survey stresses the need to ensure an adequate level of cyber resilience in the automation of the various administrative procedures, drawing some systematic implications for the same legitimacy of the use of algorithmic formulas for decision-making process.

Keywords: Artificial intelligence – Algorithmic administrative decisions – Cybersecurity – Cyber risks

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0081
Articolo sottoposto a peer review

Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act

Sebastiano Flaminio

L'articolo si propone di offrire uno spunto di riflessione sull'attuale assetto normativo sulla lotta alle fake news, con il duplice scopo di individuare gli aspetti di forza e di fragilità che i dati normativi vigenti offrono e di individuare la strada migliore da percorrere per una migliore tutela dei soggetti coinvolti. Nel corso della trattazione, si dà merito al legislatore europeo per aver predisposto la duplice proposta di regolamento del DSA e del DMA ed aver avuto il coraggio di affermare la sua sovranità in materia di rapporti digitali, con la speranza che l'*iter* di approvazione conduca anche alla valorizzazione di un approccio di governance *multi-stakeholder* per l'autoregolamentazione e all'istituzione di un'apposita autorità garante per combattere anche il fenomeno della *censura privata*.

Fake news – Info-war – Tutela dei diritti – Garante dell'informazione

Sommario: *1. Inquadramento del tema – 2. Uno sguardo preliminare: l'autoregolamentazione dei social network – 2.1. Il problema sollevato dalla giurisprudenza italiana – 2.2. L'emblematico caso di Parler – 2.3. L'estensione di una prassi pericolosa – 3. Il nuovo approccio normativo europeo: cenni sul Digital Services Act – 3.1. Uno sguardo agli ordinamenti francese e tedesco – 3.2. Uno sguardo all'esempio russo – 3.3. Una breve parentesi: l'insegnamento della politica statunitense – 3.4. L'ordinamento italiano – 4. Elementi di riflessione e spunti per l'elaborazione di una specifica disciplina: l'ambito di applicazione – 4.1. Gli strumenti di codificazione; contenuto e limiti di una possibile normativa – 4.2. Differenziazione dei profili sanzionatori – 4.3. Garanzie di tutela – 5. Una postilla conclusiva*

1. Inquadramento del tema

Come è noto, a seguito della crisi ucraina e ancor prima con i problemi scaturiti dalla gestione della pandemia da Covid-19, si è registrata una riemersione del dibattito sul tema del controllo dell'informazione e della lotta alla disinformazione nel rispetto delle libertà fondamentali e della tutela della collettività[1]. Il tema è stato oggetto di recente dibattito anche in ambito sociologico e filosofico[2], ma per comprenderne meglio i rilievi giuridici e le questioni che vi orbitano attorno bisogna allargare lo sguardo al complesso atteggiamento del nostro ordinamento verso il fenomeno della diffusione di notizie false sul Web. In questo contesto, infatti, gli ordinamenti occidentali hanno sviluppato la relativa disciplina su due direttrici: una è quella dell'autoregolamentazione, affidata direttamente alle imprese che forniscono servizi digitali, coerentemente con i modelli di governance che caratterizzano la globalizzazione; l'altra è quella delle legislazioni statali sul controllo dell'informazione. Questo secondo fronte merita adeguato approfondimento, soprattutto alla luce degli ultimi sviluppi nell'ambito delle politiche delle *big tech* volte ad affermare un pensiero standardizzato[3].

S. Flaminio è avvocato presso l'Ordine di Catania.

Nella presente trattazione sarà focalizzato lo stato dell'arte della disciplina vigente, esaminando separatamente i due versanti regolatori al fine di prospettare possibili soluzioni future a margine dell'*iter* di approvazione della nuova disciplina europea.

2. Uno sguardo preliminare: l'autoregolamentazione dei social network

Nel contesto della *network society* è cresciuta la possibilità di comunicare, in quanto la rete ha reso più veloce l'interconnessione tra individui, con la possibilità di condividere informazioni ed opinioni personali con la libertà quasi assoluta di esprimersi (anche con espressioni stravaganti). Ciò ha indotto le legislazioni di tutto il mondo a interrogarsi sulla possibilità di porre un argine agli eventuali abusi, spesso adattando le categorie giuridiche classiche ai nuovi problemi. Si pensi, ad esempio, al riadattamento delle tradizionali definizioni dei concetti di identità e di immagine alla nuova realtà in cui il paradigma della digitalizzazione è quasi un obbligo sociale.

La più evidente manifestazione delle superiori problematiche ha coinvolto la questione della regolamentazione del comportamento e del linguaggio sui social network, che sono il nuovo spazio su cui si svolge parte della vita privata e degli affari. In questo quadro, pur potendosi prospettare soluzioni giuridiche simili a quelle generalmente applicate nell'editoria, il mondo occidentale ha scelto un'altra strada, spesso generando anche insanabili contraddizioni tra il dato letterale delle norme e gli esiti dei procedimenti giudiziari. Un esempio di tale discrasia è quello per cui, mentre da un lato si prevede che una piattaforma digitale svolge un'attività esente da responsabilità per mancato controllo dei contenuti[4], ampia giurisprudenza considera le condotte diffamatorie degli utenti come illeciti commessi *con mezzo della stampa o con altro mezzo di pubblicità*.

Nel suddetto scostamento, inoltre, si inserisce l'approccio normativo euro-statunitense che ha affidato da tempo il compito di formulare le regole alle stesse imprese che gestiscono i singoli servizi digitali, delegando loro il potere di occuparsi di quella zona di rete in cui si riversa parte della vita di ognuno di noi[5]. In tale prospettiva si è aperto il dibattito sulla regolamentazione di condotte in parte inedite, sovente implicanti tutta una serie di nuovi concetti, con nuovi vocaboli e nuove figure di illecito disciplinate in modo ibrido[6]: dal cyberbullismo all'hate speech, dall'attività dei c.d. *troll* alla previsione penale sul *revenge porn*.

Sul fronte dell'autoregolamentazione, poi, la prassi insegna che le misure utilizzate più di frequente possono incidere sulla libertà di espressione tramite apparati para-sanzionatori che legittimano i social network a eliminare contenuti, sospendere le attività di un soggetto o eliminarne l'account. Tali sistemi punitivi, pur incidendo su un ambito che sovente viene ricondotto alla libertà contrattuale, non sono rimasti esenti da critiche, specie con riguardo all'impatto che gli *standard delle community* hanno sul rispetto del diritto all'eguaglianza, della libertà di parola, nonché sullo stesso "diritto" all'accesso a Internet, che meriterebbero una più approfondita analisi da parte degli ordinamenti statali[7]. Infatti, va sottolineato che la delega quasi totale che gli Stati sembrano aver concesso alle *big tech* per individuare, normare, punire, reprimere e impedire comportamenti inappropriati sul Web è foriera di evidenti ripercussioni negative sul campo del diritto, in quanto rischia di far abdicare dal potere di regolamentare e accertare gli illeciti l'unico soggetto legittimato a farlo veramente (lo Stato)[8]. È del tutto evidente, infatti, che la libertà contrattuale dei colossi di Internet deve pur sempre rispettare i limiti imposti dalle fonti normative primarie di un ordinamento.

Nondimeno, si consideri anche che la stessa attività di accertamento delle possibili condotte vietate dagli standard di un social network non è affidata a soggetti terzi e imparziali, ma a privati o ad algoritmi dal funzionamento spesso singolare e (forse) pericoloso[9]. Tali problematiche non sono di importanza trascurabile, dato che spesso hanno indotto la stessa giurisprudenza a prendere posizione per ristabilire un equilibrio tra soggetto regolatore e singoli utenti. Tra questi, meritano una breve parentesi alcuni episodi del recente passato.

2.1. Il problema sollevato dalla giurisprudenza italiana

Per meglio analizzare la problematica dell'eccessivo potere conferito alle piattaforme digitali, bisogna partire dalla considerazione che – sebbene la fonte del rapporto tra queste e l'utenza sia di origine contrattuale[10] – l'esercizio della loro facoltà di recesso spesso muta in forme di *censura privata*, ricevendo anche il biasimo della dottrina[11]. In questa fase appare utile accennare brevemente ad alcuni episodi oggetto di statuizione da parte del Tribunale di Roma[12]. In tali occasioni, il giudice capitolino ha imposto a Facebook di riattivare alcuni account, sottolineando la deduzione per cui il codice comportamentale di un social network non può scavalcare la legge, né può ritenere illeciti i comportamenti che lo stesso legisla-

tore non ritiene essere tali o, tantomeno, può presumere l'illiceità di un contenuto sgradito sulla base del mero *fumus* o delle sue scelte di politica aziendale.

Nelle pronunce cui si accennava sopra, inoltre, il Tribunale ha sottolineato anche l'importanza rivestita al giorno d'oggi da una piattaforma come quella di Zuckerberg, che ospita un numero di utenti quasi pari a un terzo della popolazione mondiale. Questa circostanza, associata al fatto che oggi non è più possibile intercettare l'attenzione di un numero altrettanto rilevante di persone su piattaforme concorrenti, rende Facebook effettivamente paragonabile ad una pubblica piazza, con le conseguenti ricadute che questo fatto ha sulle libertà garantite in Costituzione[13]. Deve concludersi, allora, che è necessario che ci sia un soggetto che vigili sulla legittimità dell'autoregolamentazione dei social network, poiché quel "potere privato" di "produrre diritto" si espone facilmente ad abusi. Inoltre, nelle parole dei giudici romani sono contenute molte risposte alle perplessità che hanno caratterizzato la materia, specie rispetto al tema della libertà di espressione[14]. Infatti, proprio in conseguenza del fatto che alcune piattaforme hanno assunto un rilievo tanto preminente, il rapporto tra queste e l'utente richiede una *speciale protezione* che non può che essere tutelata dallo Stato e dalle sue istituzioni.

Di converso, va segnalata un'ulteriore pronuncia (di segno opposto) della medesima autorità giudiziaria[15], nella quale è stato affermato che Facebook non avrebbe soltanto la facoltà di rimuovere contenuti contrari alle sue condizioni contrattuali, bensì sarebbe gravata da un vero e proprio *dovere giuridico* di rimuovere i suddetti contenuti, in virtù di obblighi di diritto internazionale. Il contrasto giurisprudenziale appena segnalato è stato oggetto di riflessione in dottrina[16], una parte della quale pare aderire al primo orientamento e criticare il secondo, in virtù della non persuasività dell'impianto argomentativo dell'ultima ordinanza citata e della scarsa appropriatezza delle norme utilizzate dal giudice romano per fondarne la motivazione[17]. Tale assunto si fonda anche sulla base di alcune statuizioni della Consulta sul rapporto tra le norme internazionali citate e la Costituzione[18], le quali legittimano i dubbi sull'ascrizione a Facebook di una *speciale posizione di garanzia* idonea a configurare una responsabilità per omesso controllo[19].

In linea di principio, allo scrivente pare più aderente ai principi del nostro ordinamento il primo dei due orientamenti giurisprudenziali[20], in quanto dallo stesso sono ricavabili due principi fondamentali: quello che qualifica lo spazio dei social network alla stregua di un luogo pubblico, con la conseguenza che chiunque può esprimere (nel limite del lecito) il suo pensiero senza costrizioni; e quello che ribadisce che la tutela ultima degli utenti non può che essere fornita da un soggetto terzo e imparziale come il giudice. Difatti, l'esigenza di tutelare gli utenti da illeciti posti in essere da altri utenti deve sempre fare i conti con l'opera di bilanciamento tra interessi contrapposti (in sede legislativa prima, in sede giudiziale poi), anche in base ai principi penalistici in tema di diritto di cronaca e diritto di critica[21].

2.2. L'emblematico caso di Parler

Non meno rilevanti, poi, sono le perplessità scaturite da un ulteriore episodio che ha coinvolto persino l'ex Presidente degli Stati Uniti ed alcuni social network, tra i quali merita menzione la piattaforma di *microblogging* di Parler. Come è noto, infatti, all'inizio del 2021 Donald Trump fu oggetto di una serie di provvedimenti di esclusione da parte di molte piattaforme. Tale evento fu seguito, prima, dalla migrazione dei suoi sostenitori sulla piattaforma di Parler e, poi, dalla rimozione della relativa applicazione dagli *store* di Google e Apple, nonché dall'oscuramento del suo sito Internet da parte di Amazon. Tali ultimi provvedimenti, che sembrano oltrepassare il limite dell'abuso di posizione dominante, furono giustificati dagli amministratori di Google e Apple con il supposto mancato adeguamento agli standard di limitazione dei contenuti che avrebbe asseritamente consentito l'organizzazione delle proteste del Campidoglio di qualche settimana prima.

Sarebbe lecito, a questo punto, chiedersi se una multinazionale abbia davvero il potere di stabilire degli standard vincolanti anche per le società concorrenti. E anche se così fosse, v'è da chiedersi come si giustifica tale potere di vincolare un altro privato e determinarne la cessazione dell'attività, senza passare dal filtro di una normativa generale e astratta, nonché dal vaglio del giudice. È del tutto evidente, infatti, che in un ordinamento democratico non è ammissibile che un privato si erga a rango di regolatore e autorità garante.

Quanto accaduto a Parler è forse uno degli esempi più estremi del problema del rapporto tra società dominanti e dominate, in quanto la decisione di escludere un'applicazione da uno *store* e spegnerne il server è del tutto affidata nelle mani della società ospitante, la quale esercita un potere sproporzionato sulla società ospite[22]. Infatti, qualora si considerasse lecita la condotta tenuta da Amazon, Apple e Google, bisognerebbe chiedersi quale qualificazione giuridica dovremmo dare a tali soggetti – soprattutto tenendo conto dell'esenzione da responsabilità stabilita dalla *Sezione 230* del *Communications Decency Act* del 1996 (omologa degli artt. 14 e 15 Diretti-

va 2000/31/CE) – in quanto nella prassi esercitano poteri e facoltà di portata considerevole[23]. V'è da chiedersi, quindi, quale sia il giusto punto di equilibrio tra potere del colosso privato e tutela dei diritti della controparte.

Quanto osservato suggerisce che probabilmente è giunto il tempo di rivedere il quadro normativo sul rapporto tra utente e piattaforme digitali, per ribilanciare le forze in campo con adeguati strumenti di tutela, anche per cercare di comprendere se l'oscuramento della piattaforma di Parler operata dalle *big tech* sia pienamente legittimo, pure in assenza di un provvedimento giudiziario[24]. Una prima risposta alle superiori problematiche, invero, è quella contenuta nel *Digital Markets Act* - DMA)[25], il cui testo sembra prossimo all'approvazione finale dopo il 5 luglio 2022. In realtà l'ambito della proposta di regolamento non coincide esattamente con l'ambito dei fatti sopra esposti, ma è comunque un importante intervento a tutela degli utenti commerciali. Senza addentrarsi nell'analisi specifica della proposta di regolamento, basti affermare che essa si è preoccupata di porre un freno alla discrezionalità con cui i *gatekeeper* limitano la libertà di impresa degli utenti commerciali (in contrasto con la libera concorrenza). A supporto del novello impianto normativo, l'Unione europea ha colto l'occasione per riappropriarsi della sovranità in quest'ambito (anche a discapito dell'azione degli Stati), proprio per poter contrastare in modo efficace e uniforme lo strapotere delle *big tech* generato dall'incapacità degli Stati di governare uno spazio così grande come quello di Internet[26]. Non sono mancati i commenti preoccupati da parte di alcune delle *big tech*[27], né quelli entusiastici di altri soggetti[28], ma ci si riserva di comprendere meglio come verrà applicata la normativa dopo le prime pronunce sui casi disciplinati al Capo III.

2.3. L'estensione di una prassi pericolosa

Da ultimo, la logica adottata dai colossi tecnologici nella vicenda di Parler ha trovato un pericoloso recepimento nel mondo reale[29]. Dopo lo scoppio della crisi russo-ucraina, infatti, i social network hanno espresso la loro posizione sul conflitto (anche cambiando politica e regole[30]), influenzando il dibattito e persino tollerando le campagne d'odio nei confronti dell'utenza russa[31]. La collettività sembra essersi subito adeguata alla politica dei social, compiendo azioni non virtuali, volte a disincentivare ogni attività ricollegabile alla Federazione Russa e ai suoi cittadini. L'aspetto più preoccupante della vicenda è che tale atteggiamento è stato assunto anche dal mondo dell'impresa, da governi nazionali, dalle borse, dagli enti sportivi e financo da enti dediti ad attività culturali come il Teatro alla Scala di Milano e l'Università Bicocca di Milano[32].

Data l'estrema polarizzazione del dibattito, riversatasi nella sua forma peggiore proprio nel mondo reale, è lecito chiedersi se non sia davvero arrivato il momento di avviare una seria riflessione sul ripristino delle regole democratiche anche su Internet, magari con adeguati percorsi formativi per il cittadino[33] e interventi volti a invertire la rotta del fenomeno della *bubble democracy*[34].

3. Il nuovo approccio normativo europeo: cenni sul Digital Services Act

All'autoregolamentazione dei social network si accompagna anche un secondo sistema (propriamente) normativo, il quale – seppure più appropriato – ha destato alcune perplessità riguardo alla tutela penalistica e alla relativa risposta punitiva verso la diffusione di notizie false. Per effettuarne un'analisi adeguata è necessario operare un confronto tra diverse esperienze giuridiche, al fine di individuarne pregi, difetti e prospettive future.

Corre l'obbligo, inoltre, di fare cenno agli ultimi sviluppi in ambito comunitario, nel cui contesto (oltre al DMA segnalato al superiore § 2.2) è stata elaborata una proposta di regolamento sul rapporto tra servizi digitali e utenza (il *Digital Services Act* - DSA), anch'essa in fase di approvazione. In linea generale, la combinazione delle due proposte di regolamento mira a proteggere in modo più efficace i diritti fondamentali degli internauti. Lo scopo precipuo del DSA, inoltre, è quello di svecchiare la normativa della Direttiva *e-commerce*, adeguando il quadro dispositivo agli sviluppi degli ultimi vent'anni e puntando a realizzare condizioni di maggior sicurezza in rete[35]. Per fare ciò la Commissione europea ha puntato proprio sulle garanzie di tutela degli utenti e della loro libertà di espressione, obbligando le *big tech* ad assumere maggiore responsabilità sui contenuti illegali o nocivi[36]. Tale scopo è raggiunto, pur mantenendo il divieto di sorveglianza preventiva, con il superamento della presunzione di neutralità delle società che operano sul Web[37]. A titolo esemplificativo, per ciò che riguarda le società di *hosting* l'art. 5, par. 1, del DSA impone di agire per rimuovere i contenuti illeciti o per disabilitare l'accesso agli stessi, non appena tali società acquisiscono la conoscenza di contenuti illeciti, decretando la fine dell'irresponsabilità dell'impresa sulla base della avvenuta conoscenza di tale attività. Ciò, però, potrebbe indurre le società di *hosting* più zelanti a disabilitare ogni contenuto che viene segnalato (senza un effettivo controllo)[38],

ma l'art. 15 della proposta sembra fornire riparo dal problema. Detta norma, infatti, sembra modellata sull'esperienza dell'obbligo di motivazione in ambito amministrativo e tributario[39], in quanto dispone (tra le altre cose) che i provvedimenti della società di *hosting* vanno motivati in modo chiaro e specifico, nonché devono contenere informazioni (facilmente comprensibili) sui mezzi di ricorso a disposizione per rendere effettivo l'esperimento dei mezzi di tutela. Questa impostazione sembra essere idonea a controbilanciare i poteri delle parti, dando all'utente la possibilità di chiarire la sua posizione e, se la limitazione è stata illegittima, la possibilità di ripristinare la situazione precedente.

Le ultime disposizioni segnalate, inoltre, vanno poste a confronto con la terza sezione della proposta di regolamento (*Disposizioni aggiuntive applicabili alle piattaforme online*), che prevede l'obbligo per le piattaforme di dotarsi di un sistema di gestione dei reclami (art. 17) e la possibilità di risolvere in via stragiudiziale le eventuali controversie (cfr. art. 18). Questo quadro appare assai vicino all'obiettivo di superare i problemi della *censura privata* e del ripianamento del dislivello contrattuale tra le parti, ma – come si dirà alla fine del presente scritto – forse l'ordinamento ha bisogno anche di ulteriori strumenti per cambiare radicalmente passo e risolvere i problemi che si stanno riversando sulla società.

3.1. Uno sguardo agli ordinamenti francese e tedesco

La normativa europea, però, non è l'unica a disciplinare il fenomeno della circolazione di notizie false. Molti ordinamenti statali, infatti, si sono occupati del tema a più riprese. In questo ambito, quindi, va posta una comparazione tra diversi ordinamenti per comprendere le differenze dei loro approcci sulla materia della lotta alla disinformazione.

In questo confronto tra le legislazioni nazionali si inserisce la Francia, la quale ha adottato un sistema sanzionatorio di tipo penalistico, principalmente disciplinato dalla *Loi du 29 juillet 1881 sur la liberté de la presse*[40], come modificata dalla *Ordonnance n° 2000-916*, la quale punisce le attività di pubblicazione, diffusione o riproduzione attraverso qualsiasi mezzo di notizie false, opere inventate, falsificate o erroneamente attribuite a terzi in malafede, che turbino o siano idonee a turbare la pace pubblica, con una ammenda di 45.000 euro, elevabile a 135.000 euro se suddette attività sono effettuate con dolo ed abbiano natura tale da minare la disciplina o la morale dell'esercito o di ostacolare lo sforzo bellico della nazione.

A tale normativa, poi, si affiancano le *Loi organique n° 2018-1201 du 22 décembre 2018* e *Loi n° 2018-1202 du 22 décembre 2018*, frutto del dibattito innescato nello stesso anno della loro emanazione. Tali normative furono pensate per arginare il fenomeno della *manipolazione dell'informazione* nei mesi che precedono le scadenze elettorali, prevedendo una pena che comporta fino a un anno di reclusione e un'ammenda di 75.000 euro in caso di violazione degli obblighi di trasparenza imposti ai gestori di piattaforme informatiche[41]. Tale disciplina, inoltre, è assistita dall'ulteriore previsione contenuta all'art. 163-2, co. 2, del *Code électoral*, il quale prevede che il giudice può ordinare (su istanza di parte) la rimozione di una notizia da una piattaforma entro quarantotto ore dalla notifica del relativo reclamo.

Da una prima occhiata, la normativa francese appare strettamente tipicizzata e finalizzata a fornire grande tutela a beni giuridici importantissimi come la pace pubblica, la disciplina dell'esercito e l'integrità dei processi elettorali. Tuttavia, ci si permette di muovere almeno una critica (comparativa) all'impianto sanzionatorio, il quale prevede solo una sanzione pecuniaria per chi minaccia la pace pubblica o ostacola lo sforzo bellico nazionale e (addirittura) una pena detentiva per la diffusione di fake news in periodo elettorale. La discrasia sanzionatoria, poi, non appare in sé proporzionata, né sembra coerente se si considera anche che la previsione della pena detentiva assiste il reato con la pena pecuniaria minore. Non sono mancate, inoltre, critiche riguardo ai possibili risvolti liberticidi del *Code électoral*[42], ma la Corte costituzionale d'oltralpe ha escluso le censure mosse dai giornalisti francesi.

Un modello alternativo a quello francese è quello tedesco che, invece, fonda la disciplina della lotta alla diffusione di fake news su uno schema diverso[43], il quale prevede (salvo specifiche deroghe) che i fornitori di servizi di telecomunicazione con più di due milioni di utenti registrati in Germania (ad esclusione dei soggetti che offrono contenuti editoriali e giornalistici) hanno il dovere di tenere un registro dei reclami contro la pubblicazione di contenuti illeciti e di gestire le segnalazioni di contenuti *manifestamente illeciti* tramite operazioni di rimozione o blocco dell'accesso agli stessi da applicare entro 24 ore dal ricevimento della segnalazione, salvi i casi in cui è permesso al gestore di dare all'utente la possibilità di replicare alla segnalazione prima che venga adottata una decisione.

A garanzia del rispetto della superiore normativa, il legislatore teutonico ha previsto anche una responsabilità di tipo amministrativo verso i gestori dei social network[44], contemplando l'inflizione di un'am-

menda che può raggiungere i 500.000 euro per le carenze organizzative e il ritardo nel riscontrare i reclami degli utenti, nonché l'ulteriore sanzione per la mancata rimozione di contenuti illeciti (fino a cinque milioni di euro). La normativa descritta ha destato alcune condivisibili perplessità sul fronte della limitazione del diritto alla manifestazione del pensiero, specie con riguardo alla pressione esercitata sul fornitore della piattaforma che – per evitare le citate sanzioni – potrebbe essere indotto a decidere di rimuovere anche i contenuti la cui liceità è solo dubbia[45].

Nonostante le menzionate criticità su entrambi i modelli, è possibile individuarne alcuni elementi di pregio; il modello francese, infatti, ha certamente il merito di aver maggiormente tipizzato le condotte punibili e di aver previsto un controllo pubblico sulla rimozione dei contenuti illeciti, mentre quello tedesco ha il pregio di aver intuito che non è necessaria una risposta punitiva di tipo penale.

3.2. Uno sguardo all'esempio russo

Le due discipline analizzate devono, inoltre, essere comparate con esperienze estranee alla tradizione occidentale. Su tanti, merita menzione il modello russo, che costituisce il modello più simile ai sistemi europei, nonostante si sia registrato il recente scivolamento della Federazione Russa dalla posizione di *democrazia imperfetta* a quella di *regime autoritario* nel 2021[46].

Per effettuare un'adeguata comparazione bisogna partire dai parametri normativi contenuti nella Legge federale n. 31-FZ del 18 marzo 2019 (che modifica l'art. 15-3 della Legge federale sull'informazione, l'informazione tecnologica e la protezione dell'informazione), e nella Legge Federale n. 27-FZ del 18 marzo 2019 (che modifica il Codice delle violazioni amministrative). Nel momento della loro emanazione, tali disposizioni hanno istituito un sistema sanzionatorio amministrativo affine a quello tedesco[47], affiancato nel 2022 da un sistema sanzionatorio di tipo penalistico più repressivo del modello francese, ma comunque vicino al prospetto normativo italiano che di seguito verrà analizzato.

Quanto al mero contenuto delle norme citate va segnalato che, formalmente al pari delle legislazioni europee, la Legge Federale n. 149-FZ prevede la piena libertà di manifestazione del pensiero, a condizione che il suo esercizio non sia finalizzato alla propaganda della guerra, all'istigazione all'odio o all'inimicizia nazionale, razziale o religiosa, nonché di ogni altra informazione dalla cui diffusione derivi responsabilità penale o amministrativa. In questo quadro normativo, la duplice riforma del 2019 ha inserito la previsione secondo cui (al pari degli editori) il proprietario dell'aggregatore di notizie è responsabile della verifica della veridicità dei fatti di rilevanza sociali da esso pubblicati[48].

A tutela del sistema di cui sopra, inoltre, già prima del 2019 era prevista la facoltà degli Enti statali o del Procuratore generale di rivolgersi al *Roskomnadzor* (organo esecutivo federale che esercita funzioni di controllo e supervisione nel campo dei *mass media*) per adottare le misure necessarie per arrestare la diffusione di contenuti vietati e l'inflizione di una multa per la pubblicazione di «informazioni false socialmente significative distribuite sotto le spoglie di messaggi attendibili che creano una minaccia per la vita, la salute o la proprietà, ovvero la minaccia di una violazione di massa dell'ordine pubblico e (o) della sicurezza pubblica, o la minaccia di ostacolare il funzionamento di strutture vitali, trasporti o infrastrutture sociali di istituti di credito, delle linee di comunicazione, dell'industria e delle imprese energetiche»[49]. Dopo la novella, il meccanismo di segnalazione e rimozione è stato esteso ai social network ed è stato trasferito all'ufficio del Procuratore generale il compito di valutare il livello di affidabilità delle informazioni ivi contenute, con lo scopo di decidere se trasmettere al *Roskomnadzor* l'istanza di adozione di misure per limitarne l'accesso. La riforma ha, inoltre, introdotto un sistema sanzionatorio pecuniario amministrativo con multe che possono raggiungere l'ammontare di un milione di rubli.

Come accennato, nel mese di marzo del 2022, è stato introdotto anche un sistema sanzionatorio penalistico per chi diffonde notizie false sulle operazioni dell'esercito russo. Tenuto conto del momento storico in cui è stata emanata la novella in discorso, può sostenersi che la *ratio* ispiratrice non sia dissimile a quella che sorregge l'art. 27 della *Loi du 29 juillet 1881 sur la liberté de la presse* e l'art. 265 del Codice penale italiano.

Si rileva, poi, che il nuovo articolo 207-3 del Codice penale russo, come introdotto dall'art. 1, co. 1, n. 1, della Legge Federale n. 32-FZ del 4 marzo 2022[50], prevede tre regimi sanzionatori (a cui sono dedicati i relativi tre commi).

Il primo di essi punisce chi pubblica o diffonde «sotto forma di rapporti affidabili» informazioni «deliberatamente false contenenti dati sull'uso delle forze armate della Federazione Russa allo scopo di proteggere gli interessi della Federazione Russa e dei suoi cittadini, mantenere la pace e la sicurezza internazionali», con varie sanzioni pecuniarie (multa da settecentomila a un milione e mezzo di rubli, multa pari a «l'importo del salario o dello stipendio, o qualsiasi altro reddito della persona condannata per un

periodo da un anno a diciotto mesi») o con la condanna fino a un anno di «lavoro correttivo» o fino a tre anni di «lavoro obbligatorio», nonché l'eventuale reclusione fino a tre anni.

Il secondo comma prevede un regime aggravato con cui si sanziona il soggetto che commette il fatto di cui sopra approfittando della sua «posizione ufficiale», o agendo in concorso con altri o all'interno di un «gruppo organizzato», o per motivi «egoistici» o per «odio politico, ideologico, razziale, nazionale o religioso, o verso qualsiasi gruppo sociale», ovvero creando artificiosamente «prove per l'accusa», con una multa da tre a cinque milioni di rubli o coincidente con importo del reddito percepito in un periodo da tre a cinque anni, o con il «lavoro forzato» per un periodo massimo di cinque anni, ovvero con la reclusione da cinque a dieci anni, nonché l'interdizione dal «ricoprire determinati incarichi o impegnarsi in determinate attività» fino a cinque anni.

Infine, il terzo comma prevede un reato di danno, seppure espresso con un linguaggio assai indeterminato, con cui si punisce il reo che abbia «cagionato gravi conseguenze» con la pena alla reclusione da dieci a quindici anni e l'interdizione dal ricoprire incarichi o svolgere professioni per un periodo massimo di cinque anni.

Pur non condividendo la scelta di una previsione penalistica, va posto l'accento su alcuni aspetti che sembrano di poter essere apprezzati. È indubbio, infatti, che la puntuale tipizzazione delle ipotesi di illiceità che comportano la risposta punitiva ha senz'altro il pregio di aver stabilito un preciso ambito della normativa contro la disinformazione, con l'ulteriore merito di aver affidato i controlli a soggetti almeno astrattamente terzi e imparziali[51] come la Procura generale e il *Roskomnadzor* (che altro non è che un ente garante alla stregua dell'omologa italiana Commissione di vigilanza per i servizi radiotelevisivi). Il fatto che la Federazione Russa non rappresenti il modello ispiratore delle democrazie occidentali, infatti, non sottrae pregio alla scelta di strutturare un settore tanto delicato dell'ordinamento con fattispecie tipiche affidate al vaglio di autorità pubbliche[52]. Altro elemento di pregio, poi, è l'associazione della sanzione più grave a illeciti di danno. Quanto alla risposta sanzionatoria, infine, va segnalato che il sistema russo contempla comunque un prospetto edittale del tutto paragonabile (e a tratti più tenue) a quello cui ricorre attualmente il legislatore italiano.

3.3. Una breve parentesi: l'insegnamento della politica statunitense

Con la circostanza per cui la disinformazione costituisce «una minaccia per la sicurezza pubblica» segnalata dal riformatore russo del 2019[53] sembrano concordare anche gli USA[54]. In questo solco, infatti, si inseriscono tutti gli interventi di *cybersecurity* portati avanti dall'amministrazione americana degli ultimi anni[55], nel cui contesto va inclusa anche l'istituzione, presso il Dipartimento per la sicurezza interna, del tanto discusso Comitato per la governance della disinformazione (*Disinformation Governance Board*)[56], il quale avrebbe dovuto prevenire la diffusione di notizie false attraverso la rete. "Avrebbe dovuto" si è detto, perché solo dopo tre settimane dalla sua istituzione l'organismo è stato sospeso a causa delle polemiche causate dalla poca chiarezza sui suoi obiettivi[57].

Tali polemiche, invero, non erano del tutto inaspettate. Già in passato, infatti, si era notato che il fenomeno della disinformazione online sta conducendo gli ordinamenti occidentali a un rovesciamento della cultura politica in tema di libertà di espressione e al ribaltamento delle posizioni degli stessi attori della politica[58]. Come evidenziato già in tema di *bubble democracy*, inoltre, è stato evidenziato come la disinformazione venga utilizzata anche da governi democratici a scopi propagandistici, con la conseguenza di condizionare l'opinione pubblica e indurla a mostrare intolleranza verso le "idee diverse"[59]. Tutti vizi, questi, che rischiano di far incappare i sistemi occidentali negli stessi problemi sostanziali che macchiano l'esperienza dei regimi non liberali.

Come osserva Andrea Mazziotti di Celso, affidare il controllo sulla disinformazione «all'autorità costituita può essere molto pericoloso quando, come nel caso delle notizie politiche, governo, maggioranza (e talvolta anche i giudici) hanno un interesse diretto nella questione». Tuttavia, tale posizione non appare condivisibile *in toto*, in quanto l'errore americano non è stato tanto quello di istituire un'autorità *ad hoc*, quanto quello di prefiggersi degli obiettivi troppo ampi con un approccio divisivo. Invero, l'esperienza americana deve insegnarci che un'eventuale autorità garante non deve fungere da mero *giudice del vero e del falso*, bensì dovrebbe occuparsi di vagliare solo la veridicità di fatti (e non anche di comportamenti, opinioni, posizioni politiche etc.), perché il rischio di censura inquina il dibattito al pari della disinformazione.

L'idea di istituire un'autorità garante, infatti, andrebbe vagliata seriamente per la sopravvenuta necessità di combattere tre fenomeni opposti, ma

ugualmente insidiosi, rispetto alla diffusione di fake news: la *censura privata*, la creazione di *giudici privati*, nonché la mancanza di terzietà dei *fact-checkers* e degli algoritmi[60]. Pertanto, nel delineare i caratteri che dovrebbero tratteggiarne tale figura, il legislatore dovrebbe seguire rigidi parametri: l'autorità deve essere pubblica, ma indipendente dal governo; deve essere caratterizzata dall'assenza di conflitti d'interessi con le parti coinvolte; la sua azione deve riguardare esclusivamente fatti verificabili; i suoi membri devono avere determinate caratteristiche tecniche e il rinnovo degli incarichi non deve corrispondere con le scadenze elettorali; le sue decisioni devono essere impugnabili davanti all'autorità giudiziaria.

3.4. L'ordinamento italiano

Tornando all'analisi comparativa tra ordinamenti europei, si rileva che il tema della lotta alla disinformazione non è sconosciuto in Italia, ove vige una normativa con radici risalenti e assai più frastagliata di quella di altri Paesi. Nonostante la novità del tema delle fake news, infatti, non può trascurarsi in fatto che il nostro legislatore ha già affrontato la tematica a più riprese, tanto al tempo della codificazione degli anni Trenta del Novecento, quanto in tempi più recenti. E ciò non solo a tutela dei diritti del singolo[61], ma anche a tutela del pubblico interesse e della collettività.

Nel dettaglio, pur non trascurando di menzionare l'introduzione di appositi delitti[62] e la previsione di aggravanti associata all'utilizzo di nuove tecnologie[63], già nell'originario Codice Rocco erano previsti reati comuni che punivano la pubblicazione e diffusione di *notizie false, esagerate o tendenziose*. Per mera scelta espositiva, si procede all'esame del contenuto della citata disciplina in ordine al tipo e all'entità della risposta punitiva, dalla meno invasiva alla più repressiva.

Si analizza, pertanto, la previsione di cui all'art. 656 c.p., che prevede una contravvenzione che contempla l'alternativa punitiva tra l'arresto fino a tre mesi e l'ammenda fino a 309 euro per chiunque «pubblica o diffonde notizie false, esagerate o tendenziose». In questa sede è giusto il caso di evidenziare che si tratta di un reato di pericolo, con il quale si punisce il mero rischio di turbare l'ordine pubblico[64].

Parzialmente diverso è il discorso relativo all'art. 501 c.p., che prevede una figura delittuosa che punisce con la pena della reclusione fino a tre anni e con la multa da 516 a 25.822 euro (oltre l'interdizione dai pubblici uffici) chiunque «pubblica o altrimenti divulga notizie false, esagerate o tendenziose o adopera altri artifici atti a cagionare un aumento o una diminuzione del prezzo delle merci, ovvero dei valori ammessi nelle liste di borsa o negoziabili nel pubblico mercato» con il fine specifico di turbare il mercato interno. Anche in questo caso si tratta di un reato di pericolo, salvo intervento dell'aggravante prevista al comma 2 per i casi in cui «l'aumento o la diminuzione del prezzo delle merci o dei valori» si verifica realmente. Inoltre, il delitto in esame è perseguito anche se il fatto è commesso all'estero quando punta a danneggiare la valuta nazionale o titoli pubblici italiani. Sul piano degli aumenti di pena, infine, la risposta punitiva è raddoppiata se il delitto è commesso per favorire interessi stranieri o se da esso deriva un deprezzamento della valuta nazionale o dei titoli dello Stato, o il rincaro di merci di comune o largo consumo.

L'ultima (e non meno importante) disposizione sopra segnalata è l'art. 265 c.p., che prevede il delitto di *disfattismo politico* e punisce chiunque *in tempo di guerra*[65] diffonde o comunica «voci o notizie false, esagerate o tendenziose, che possano destare pubblico allarme o deprimere lo spirito pubblico o altrimenti menomare la resistenza della nazione di fronte al nemico, o svolge comunque un'attività tale da recare nocumento agli interessi nazionali», stabilendo la pena della reclusione non inferiore a cinque anni. Il delitto, poi, è aggravato in talune ipotesi, per le quali il codice prevede la pena della reclusione non inferiore a quindici anni se il fatto è commesso tramite propaganda, è diretto a militari o se il reo ha agito in seguito a intelligenze con lo straniero, nonché la pena dell'ergastolo se il reo ha agito in seguito a intelligenze col nemico.

Ciò detto, bisogna dar merito alla normativa italiana per aver ampiamente tipizzato e circostanziato la risposta punitiva tra più livelli di tutela, ma va altresì segnalato che l'attuale sistema presenta alcune criticità.

Infatti, il quadro normativo delineato è sicuramente applicabile all'ambito entro cui operano i social network e i motori di ricerca[66], in quanto essi sono lo strumento sempre più utilizzato per attingere alle informazioni e i loro algoritmi sono strutturati in modo tale da indirizzare l'utente verso determinate informazioni (tanto da essere stati anche oggetto di scandalo e preoccupazioni per la tenuta delle democrazie[67]). V'è da chiedersi, pertanto, se risulta punibile anche il gestore delle piattaforme che programma tali algoritmi, generando un cortocircuito con l'attuale principio di neutralità del servizio di hosting.

Quanto alle modalità di protezione del bene pubblico, poi, va segnalato che quasi tutte le fattispecie evidenziate non riparano la società da un danno concreto, bensì anticipano la tutela penale al momento

in cui potrebbe manifestarsi il mero rischio di verificazione del danno stesso. Questa circostanza rischia di dare una risposta eccessiva ai fenomeni che caratterizzano l'ambiente tipico dei social network, nei quali la maggior parte delle *condivisioni* non sono precedute da approfondimento e analisi speculativa[68], ma dipendono da estreme semplificazioni e *tendenze* dettate dagli algoritmi stessi[69]. Pertanto, si rischia di non comprendere più le ragioni dell'equiparazione tra chi *pubblica* consapevolmente una notizia falsa e chi semplicemente *diffonde* con un *click* la stessa notizia[70], senza averne degnamente approfondito il contenuto[71].

3.4.1. Tentativi di riforma

Più di recente, la materia è stata oggetto di proposte di riforma che, pur nella nobiltà dei propositi ispiratori di una disciplina di dettaglio, hanno fatto emergere l'inadeguatezza dello spirito risolutivo del legislatore italiano, più concentrato a scorgere elementi emergenziali anziché rinvenire soluzioni strutturali. Nello specifico ci si riferisce ai disegni di legge Gambaro e Zanda-Filippin[72].

Per l'analisi completa delle problematiche scaturite dalle suddette proposte legislative si rimanda alle più lucide analisi già formulate da altri. In questa sede si riporta solo che la dottrina ha ritenuto le proposte del 2017 non idonee a combattere la disinformazione, in quanto gli strumenti prospettati erano confliggenti con i principi di proporzionalità ed efficacia, oltre a decontestualizzare la disciplina rispetto ai fenomeni sottesi[73]. Pare essere diffusa poi l'idea per cui il *ddl Gambaro* violasse i principi di determinatezza, tassatività e offensività[74], oltre a contrastare con la libertà di manifestazione del pensiero «in nome di un sinistro richiamo allo Stato Etico di matrice totalitaria»[75]. Dal testo del ddl, inoltre, sembravano emergere anche alcuni problemi in relazione all'imputabilità del fatto, apparendo almeno curioso che il legislatore – a fronte della previsione di nuovi reati comuni – avesse inteso esentare dai nuovi profili di responsabilità proprio i giornalisti e i quotidiani online[76], nonostante le previsioni di cui agli artt. 3 e 7 sembrassero tradire l'intenzione di compiere un passo verso l'omogeneizzazione della posizione dei social network rispetto a quella degli editori. Non si trascuri, poi, che una tale previsione era priva di senso, in quanto anche i professionisti dell'informazione possono incorrere in errore o frettolosamente riferire fatti non verificati[77] e, proprio per la loro speciale posizione, sono tenuti a rispettare con maggior rigore le regole rivolte al cittadino comune.

In chiusura, appare utile ribadire che il problema della disinformazione non può essere risolto con la mera minaccia di sanzioni penali, né può ritenersi utile l'abdicazione del controllo della rete da parte dello Stato in favore dei privati[78]. Ed invero, qualora la sanzione penale si rivelasse l'unico strumento di tutela efficace, sarebbe opportuno tenere fermi due punti: anzitutto, dovrebbe prediligersi la formulazione di reati di danno; in secondo luogo, ove il legislatore volesse contrastare il mero pericolo di lesioni al pubblico interesse, dovrebbe ricorrere a sanzioni amministrative, interdittive e deontologiche.

4. Elementi di riflessione e spunti per l'elaborazione di una specifica disciplina: l'ambito di applicazione

Con gli elementi sin qui raccolti è possibile tracciare la base per una prospettiva di riforma che tenga conto dei pregi e delle perplessità presenti nelle legislazioni sopra menzionate, nonché degli ultimi sviluppi dell'ordinamento europeo. Per meglio evidenziare i punti su cui insistere, però, è opportuno suddividere l'analisi su quattro direttrici: l'ambito applicativo; gli aspetti riguardanti la puntuale codificazione; la differenziazione della risposta punitiva; gli strumenti che rendono effettiva la tutela degli interessi contrapposti.

Sul primo profilo, è di immediata comprensione che Internet è uno spazio diverso dal mondo reale ed è costellato da opportunità e insidie. In una rete senza confini spaziali e temporali, quindi, l'ambito applicativo di una disciplina contro la diffusione di fake news deve essere approntata da un legislatore consapevole della complessità del contesto in cui si opera e dotato degli strumenti che gli permettano di intervenire. Una tale sfida non può che essere affrontata tramite lo strumento dell'extraterritorialità o con la previsione concordata tra più Stati di un'unica disciplina[79] (come del resto sta già accadendo con le proposte di regolamento dei DMA e DSA). Infatti, l'ambito applicativo di una possibile normativa che si prefissi lo scopo di lottare contro la disinformazione sul Web non può che spiegarsi su un panorama più diffuso possibile. E ciò non solo per fornire tutela all'utente dalla minaccia esterna al territorio nazionale[80], ma soprattutto per dotare la comunità di regole omogenee e adatte alla mobilità tipica della globalizzazione[81].

Appare scontato, pertanto, che il nostro ordinamento necessiti di strumenti ottenibili tramite una disciplina comunitaria o con cooperazioni rafforzate che rendano più omogenee possibile le regole appli-

cabili alla materia della tutela del singolo e della comunità della rete, non trovando giustificazione una risposta punitiva eccessivamente differenziata e parcellizzata per fatti identici commessi in luoghi diversi. È stata proprio quella parcellizzazione, infatti, che ha causato la nascita di centri di *potere privato* che oggi vanno arginati.

Risolta nel più ovvio dei modi la prima delle quattro questioni, non resta che analizzare più approfonditamente le successive direttrici.

4.1. Gli strumenti di codificazione; contenuto e limiti di una possibile normativa

Dal punto di vista degli strumenti normativi da utilizzare, si è già detto della predilezione di fonti di rango primario o internazionale[82], che (a differenza delle norme di *soft law*) hanno il duplice vantaggio della maggior ponderazione e di essere sottoponibili al vaglio della Consulta. Non va dimenticato, infatti, che la questione della lotta alle fake news si trova pur sempre in quello scivoloso crinale che separa la libertà di manifestazione del pensiero dalla necessità di proteggere beni giuridici altamente rilevanti: quindi, senza un adeguato bilanciamento e senza la vigile attenzione di organi come la Consulta il rischio è quello di incorrere in pericolose storture del sistema[83].

Tuttavia, ciò non significa che il tema debba essere affrontato esclusivamente da norme di rango primario, in quanto la mutevolezza dei fenomeni nell'era di Internet rende necessaria un'alleanza tra il legislatore e le piattaforme digitali. Pertanto, è opportuno che l'eventuale riserva di legge in materia abbia natura relativa, al fine di lasciare tutte quelle valutazioni che esulano dal bilanciamento, dal piano sanzionatorio e dalla risoluzione delle controversie, nelle mani degli enti che si interpongono tra lo Stato e l'utente[84]. In estrema sintesi, potremmo definire gli spazi destinati alla normazione dei due soggetti coinvolti in base al rapporto che si intende tutelare nel seguente modo: da una parte, lo Stato deve occuparsi di disciplinare il rapporto tra imprese che gestiscono servizi telematici ed utenza (almeno la parte con le maggiori ricadute sociali), mentre i social network devono limitarsi a tutelare l'utente dai fatti lesivi causati da altri utenti (compresi i c.d. *cracker*, *hater*, *cyber-stalker* o gli autori di attacchi malevoli tramite *fishing*, *ransomware*, etc.).

Definiti gli ambiti entro cui i due livelli normativi dovrebbero impegnarsi, non va trascurata una seconda differenza che il legislatore e le *big tech* sono tenuti ad osservare per l'individuazione dell'oggetto della materia di cui si discute: la distinzione tra cronaca e critica. Non è un problema di secondaria importanza, infatti, quello che emerge direttamente dalle linee-guida dei social network, le quali trattano alla stessa stregua la diffusione di *fatti non veri ed opinioni meno condivise*, disinteressandosi del fatto che in un caso si tratta di false attestazioni di fatti inesistenti, mentre nell'altro caso ci sono evidenti ricadute sulla libera manifestazione del pensiero.

Giova a questo punto tracciare il confine tra i due concetti con un'analisi logico-semantica che affonda le sue radici sulla sostanziale differenza tra *fatto* e *opinione*. Ebbene, con il termine *fatto* si indica un «avvenimento, azione, fenomeno, ciò che si compie o si è compiuto [...] già avvenuto, che non può quindi più essere impedito o modificato, davanti al quale non resta che troncare ogni questione»[85]; nel suo significato generico, il termine identifica «ciò che ha consistenza vera e reale, in opposizione a ciò che non è concreto, tangibile, sicuro». Pertanto, tutto ciò che è un *fatto* è indiscutibilmente reale, esistente e tangibile. Nettamente diverso, invece, è il significato del termine *opinione* (dal verbo latino *opinari*[86]), il quale esprime un «concetto che una o più persone si formano riguardo a particolari fatti, fenomeni, manifestazioni, quando, mancando un criterio di certezza assoluta per giudicare della loro natura (o delle loro cause, delle loro qualità, ecc.), si propone un'interpretazione personale che si ritiene esatta e a cui si dà perciò il proprio assenso, ammettendo tuttavia la possibilità di ingannarsi nel giudicarla tale». L'*opinione* si contrappone al *fatto certo*, perché rappresenta la convinzione che un soggetto ha riguardo ad un determinato fatto ed esprime un giudizio di valore (come con le *opinioni prevalenti* in dottrina) o un modo di pensare collettivo (la c.d. *opinione pubblica*, che può dipendere da «esigenze, convinzioni, atteggiamenti mentali comuni», nonché da pregiudizi e convenzioni sociali). È ovvio, quindi, che la lotta alle fake news debba limitarsi alla verifica di pubblicazioni che riferiscono esclusivamente *fatti*, non potendo in alcun modo mettere al bando l'esposizione di *opinioni*. Ciò si traduce in termini giuridici nella distinzione tra il diritto di cronaca e il diritto di critica, in quanto il primo trova limite nella verità dei fatti esposti, mentre il secondo trova limite solo nella forma e nel rispetto dell'altrui dignità[87].

Pertanto, la disciplina della materia di cui si tratta deve avere ad oggetto solo il primo dei due profili sopra esposti. Essa dovrebbe, nondimeno, concedere anche la possibilità di diversificare il panorama della diffusione di notizie, senza gli impropri automatismi generati dagli algoritmi[88] e distinguendo tra la rimozione di notizie false e la contestabilità di notizie controverse. Ciò potrebbe ottenersi con un ventaglio di soluzioni, tra cui la sottoposizione a segnalazione dei

contenuti controversi (tramite un avviso all'utente) e a eliminazione di contenuti illeciti, pur senza sottrarsi dalla prospettiva di riabilitare il soggetto che in passato ha violato le regole[89]. Tuttavia, per non incorrere negli stessi problemi della legge tedesca, è opportuno diversificare anche la tipologia dei provvedimenti predisponibili dai social network. Difatti, non va trascurato il fatto che oggi la possibilità di interagire nel Web è di cruciale importanza per compiere operazioni necessarie per lo sviluppo sociale, economico e politico del singolo[90]. Quindi, il rapporto tra social network e utenza non può più ridursi al mero aspetto contrattuale, ma va considerata la *speciale posizione* assunta dal soggetto più forte al quale va richiesto di «attenersi al rispetto dei principi costituzionali e ordinamentali finché non si dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente»[91].

Pertanto, va elaborato un sistema che non impedisca *in perpetuo* l'accesso del trasgressore ad una piattaforma, ma limiti semplicemente le sue interazioni con terzi per un tempo ragionevole che permetta di presumere che non verranno poste in essere ulteriori violazioni in futuro. Infatti, la sospensione della possibilità di pubblicare una notizia falsa (tramite la momentanea inibizione della facoltà di pubblicare alcunché) è già una misura sufficiente a *correggere* il comportamento della generalità degli utenti[92]. Da ciò discende, che il legislatore dovrebbe fortemente limitare la possibilità del soggetto dominante di recedere unilateralmente dal servizio[93], in ossequio alla tutela dello sviluppo personale e sociale degli utenti e in considerazione del fatto che non è più possibile svolgere una parte importante della propria vita al di fuori della rete.

Tali operazioni, poi, non vanno compiute dagli algoritmi, ai quali andrebbe affidato solo il compito di limitare la possibilità di reperire contenuti che – seppure leciti – risultano inadatti per alcune fasce di utenza (come già avviene con gli strumenti del *parental control* o di YouTube Kids, che offrono protezione ai minori pur non privandoli della possibilità di usufruire dei servizi telematici).

Infine, non va trascurata l'ulteriore esigenza di regolare con precisi limiti la facoltà para-normativa degli stessi social network, la quale spesso si è prestata a piegare la logica del pluralismo a quella del condizionamento[94], insistendo nell'opera di persuasione volta a modificare le opinioni di chi non rientra in una determinata *bolla*, tramite l'isolamento (*ban*, limitazioni dei contenuti e delle interazioni), premi e privazioni (direzionando i contenuti verso platee più o meno ampie, permettendo di avere più visualizzazioni e reazioni, in base alla linea seguita da un *post* e alle *tendenze*) col preciso scopo di provocare l'abbandono degli originari convincimenti e l'adesione necessitata ad una fazione. In questo senso, allora, la norma primaria deve necessariamente fungere da cornice edittale entro cui le piattaforme digitali devono muoversi nello stabilire quali contenuti siano ammissibili al loro interno, per tutelare il pluralismo e la corretta formazione di opinioni. Infatti, la lettura distorta (ma ammessa) di un fatto vero è tanto pericolosa quanto la diffusione di notizie false, in quanto influenza la percezione del lettore in egual misura e desta le preoccupazioni di chi vede un pericolo nei fatti emersi nel superiore § 2.3. Pertanto, anche su questo fronte, l'ordinamento deve stabilire precise regole e profili di responsabilità per i social network che violano il principio pluralista, oltre a dare eccessiva visibilità ad una prospettiva di lettura e limitano lo spazio concesso a punti di vista differenti[95].

4.1.1. Una sede per il confronto tra gli attori del sistema

Le superiori argomentazioni richiedono anche una breve postilla in merito alla cooperazione tra ordinamento e multinazionali. Per meglio comprendere quanto si sosterrà in questa sede, è necessario compiere una brevissima premessa con le parole di un filosofo del diritto e di uno storico del diritto. Il primo ha sostenuto che i sistemi di governance e il *soft law* rischiano di dare troppo potere ai pochi, a detrimento dei diritti dei molti. In questo quadro, descritto come un *ritorno al futuro*, l'autore esprime tutte le sue preoccupazioni per le possibili violazioni dei valori ereditati dalla modernità[96]. Il secondo, invece, pur confermando l'idea di quel ritorno ad una *medievalità giuridica* (ovvero al sistema interconnesso di fonti diverse), non pare mostrare le stesse perplessità, intravedendovi piuttosto lo spunto per un'ulteriore evoluzione dell'attuale sistema giuridico[97]. Nonostante la diversa lettura, col senno di poi si può sostenere che entrambi hanno avuto ragione: il primo nell'intuire i pericoli della tecnocrazia da cui è derivata la *censura privata*; il secondo nel comprendere che questo scenario è solo un passaggio temporaneo (ma necessario) per costruire nuovi scenari.

Ebbene, si è già accennato ai problemi di impianti normativi di *soft law* come il *Code of Practice on Disinformation* e del relativo sistema di *governance* che pare «delegare interamente alle Internet platforms i tentativi di regolamentare [...] rinunciando a qualsiasi tipo di controllo sulla sua efficienza e correttezza»[98] e causando seri rischi per la libertà di espressione[99]. Ciò non significa che il fenomeno della

disinformazione non vada combattuto o che la collaborazione tra Stato e multinazionali sia un fenomeno da respingere del tutto, ma si rileva che bisogna agire «senza tuttavia delegare poteri eccessivi e arbitrari a corporation che gestiscono senza nessun quadro legislativo a tutela della libertà di informazione (e di espressione)»[100] e, soprattutto, senza sfociare in improbi conflitti tra potere pubblico e *poteri privati*[101] o costituire pericolose forme di *giudici privati*[102].

Alla luce di ciò, allora, bisogna chiedersi se non sia possibile ribilanciare lo squilibrio tra l'utente e le piattaforme proprio partendo dalle mancanze dei sistemi di *soft law*. E pertanto, posto che le deleghe ai privati e i sistemi di *soft law* hanno generato rilevanti problemi in tema di libertà e democrazia, esistono strumenti alternativi per recuperare quella dimensione democratica? Una risposta positiva sembra potersi trarre dall'esperienza della governance *multi-stakeholder* brasiliana, la quale pare aver dimostrato che un approccio improntato sul confronto democratico può contribuire ad un miglioramento del rapporto tra gli attori del "vivere digitale"[103].

Ma un confronto tra molteplici attori richiederebbe una sede adatta al componimento dei conflitti che il dibattito inevitabilmente genera: e allora, quale sarebbe la sede più adatta? A questo punto del discorso, meriterebbe maggiore attenzione il tema degli organi ausiliari che, nell'esperienza dello Stato sociale, aveva trovato come sede del confronto tra classi i consigli economico-sociali. Lo Stato sociale, infatti, in quanto "fondato sul lavoro" aveva trovato in essi la sede opportuna per ricomporre le crisi sociali[104]. Lungi dall'impelagarsi in un excursus eccessivamente lungo, basti in questa sede riportare che, tanto in Italia (nel 1948), quanto in Francia (prima nel 1946 e poi nel 1958), in Olanda (nel 1950), nella Comunità europea (già nella sua fase embrionale, nel 1958) e persino in Spagna (nel 1991) e Irlanda (nel 2006) sia stata riproposta la medesima idea. Tutte esperienze che, in un modo o nell'altro, hanno aderito ad una tendenza che pare aver caratterizzato una specifica forma di Stato. Ai fini del presente scritto, tutte le superiori premesse conducono, quindi, alla possibile istituzione di una sede del confronto in sede europea che sarebbe opportuno affidare al Comitato economico e sociale europeo (similmente a quanto già accade in diverse materie individuate dal TFUE) sulla base del fatto che, così come un consiglio economico è luogo idoneo a realizzare gli scopi di coesione e solidarietà di uno Stato sociale, allo stesso modo una sede istituzionale del confronto tra i possibili *stakeholder* (Stati, multinazionali, utenti, tecnici etc.) è il luogo idoneo per ricucire gli eventuali conflitti tra gli attori in gioco.

Qualora un tale confronto fosse troppo artificioso o inefficace, l'alternativa potrebbe essere quella di sostituire la delega alle multinazionali tipica del sistema di *soft law* con una sorta di "contrattazione collettiva" o intese multilaterali (tra Stati, multinazionali, associazioni di consumatori, tecnici del settore ed esperti in materie giuridiche) per la fissazione dei limiti alle modalità di esercizio del potere privato delle piattaforme stesse. Tale alternativa, però, dovrebbe essere accompagnata dalla previsione di una norma imperativa che disponga anche la "nullità ad ogni effetto" delle intese che limitano la libertà di parola, al pari di quanto già accade nella disciplina in materia di antitrust[105]. Difatti, così come la concorrenza è un valore fondamentale nella disciplina della tutela del mercato, la libera manifestazione del pensiero è un principio imprescindibile nel contesto della presente trattazione.

4.2. Differenziazione dei profili sanzionatori

Quanto alle tutele civili e penali offerte dagli Stati, vanno analizzate alcune problematiche che meritano separata analisi.

In ambito civile, infatti, vanno considerati i profili di certezza, rapidità ed efficacia della tutela. Su questo fronte va lodato lo sforzo del legislatore nazionale, che (anche a causa dell'aumento dei processi[106]) ha ricompreso nella disciplina sulla mediazione anche le controversie in materia di diffamazione a mezzo stampa[107]. Ma sul Web tali regole richiedono ulteriori adeguamenti perché spesso risultano insufficienti o eccessive. Per spiegare meglio l'ossimoro bisogna considerare le contrapposte esigenze del soggetto segnalante e del soggetto segnalato. E infatti, per tutelare efficacemente il segnalante anche dalle condotte più insidiose (come nel caso in cui lo stesso social network non elimini il contenuto illecito che, però, non viola gli *standard della community*) servirebbe un'apposita *obbligazione di garanzia* delle piattaforme (in veste di sanzione civile) che determini una sua responsabilità solidale a garanzia dell'utente che si trova costretto ad adire l'autorità giudiziaria[108]. Dall'altro lato, però, va considerato che il soggetto che subisce l'ingiusta cancellazione di un contenuto lecito merita altrettanta tutela. Egli, invero, potrebbe trovarsi a subire una segnalazione per aver destato solo il fastidio del segnalante, pur senza aver leso in alcun modo un suo diritto (come nel caso dell'artista che pubblica un'opera che contiene nudità e subisce una segnalazione per contenuti pornografici). Per tutelare le sue prerogative, allora, bisogna riequilibrare il rapporto tra utente e piattaforma, disciplinando uno speciale procedimento davanti ad un'apposita

autorità garante[109], i cui provvedimenti costituiscano prova privilegiata contro il social network tanto ai fini della verifica della liceità del contenuto rimosso (per ripristinarlo) quanto ai fini dell'eventuale causa di risarcimento del danno[110].

A fare da ombrello a entrambi gli utenti di cui sopra e da deterrente per l'approssimazione delle regole dei social network, quindi, l'ordinamento deve premunirsi di strumenti adeguati che permettano di rimuovere rapidamente contenuti palesemente illeciti o permettano un immediato chiarimento e il ripristino di quelli leciti, evitando la proliferazione di giudizi sulla questione. Una risposta in tal senso pare essere tra gli scopi del DSA, il quale prevede proprio delle facilitazioni per l'utente che voglia accedere a forme non giudiziali di risoluzione della controversia[111].

Sul fronte penalistico, poi, bisogna muovere delle serie critiche alle legislazioni vigenti che spesso appaiono tendenti a reprimere il fenomeno della diffusione di fake news con sanzioni eccessive. Tali aspetti di criticità discendono spesso dal contesto emergenziale in cui vengono approntate le maggiori novità normative, o da una tradizione troppo vetusta per rispondere alle esigenze di dinamicità dei fenomeni discendenti dalla globalizzazione, sicché pare necessario che un'eventuale novella predisponga un quadro sanzionatorio diversificato ed adeguato alle novità del tempo, senza compiere necessariamente la scelta radicale di ricorrere alle sanzioni penali per *correggere* l'evoluzione della società. Pertanto, il parametro principale della presente riflessione deve essere il bene giuridico che si vuole tutelare con la lotta alle fake news, che è non già il mero diritto ad essere informati, quanto invece il diritto ad essere *correttamente* informati, evitando di incorrere in episodi di diffamazione o di minaccia dell'ordine pubblico.

Sotto il profilo dell'individuazione di nuove fattispecie, poi, non va trascurato un altro aspetto che nel recente passato il legislatore non ha adeguatamente considerato: si tratta della differenza tra chi pubblica *ex novo* una notizia e chi la diffonde tramite *condivisione*[112]. La differenza è di non poco conto nell'ambito virtuale, in quanto spesso l'utente medio condivide link con estrema leggerezza[113]. In questo contesto, inoltre, va fatta l'ulteriore distinzione tra chi pubblica in malafede una notizia che sa essere falsa e chi pubblica una notizia sulla base di una falsa percezione di fatti o nell'erronea convinzione che sia vera[114]. Tali differenziazioni sono cruciali nell'epoca delle *infodemie* e richiedono una puntuale applicazione del principio di frammentarietà. Solo dopo aver sciolto questi nodi sarà possibile delineare i profili di un'eventuale novella.

La responsabilità penale, infatti, è la più estrema manifestazione del potere punitivo dello Stato e può essere oggetto di specifica previsione solo quando è altrimenti impossibile impedire la minaccia ad un determinato bene giuridico (c.d. *extrema ratio*). Quindi, difronte a tali considerazioni è opportuno che il legislatore provveda a risolvere il problema dell'adeguamento delle sanzioni in due direzioni: da una parte, dovrebbe effettuare una più approfondita differenziazione dei soggetti agenti come sopra delineati, per rispecchiare sul piano normativo il reale contesto sociale di Internet; dall'altra, invece, dovrebbe effettuare una maggiore differenziazione dei casi di responsabilità penale per la diffusione di notizie false con una corrispondente graduazione della pena.

4.3. Garanzie di tutela

Non meno trascurabile, poi, è il profilo degli strumenti da porre a garanzia dell'effettività della tutela degli interessi che si scontrano al confine tra il diritto di esprimersi e il dovere del rispetto altrui. Nello scenario delineato dalla normativa vigente, infatti, non di rado si è riflettuto sul riequilibrio di posizioni giuridiche che appaiono inconciliabili.

In questo contesto, il primo problema da risolvere è quello dell'individuazione dei soggetti che dirimano le controversie che insorgono. Spesso, infatti, si è già dubitato dell'imparzialità dei *fact-checker* e degli algoritmi[115], ma la questione non è impossibile da risolvere. Infatti, si è ipotizzato di affidare il compito di verificare la correttezza delle informazioni a un'autorità pubblica e terza. È un pensiero criticato[116], ma non del tutto isolato[117].

Riteniamo che la verifica della liceità di un *contenuto on line* debba essere affidata a soggetti che non abbiano conflitti di interessi, come invece sarebbe se si affidasse a singole testate giornalistiche il compito di compiere operazioni di *fact-cheking* dei contenuti di altre testate. Tale problema sarebbe risolvibile tramite la previsione di un'autorità i cui membri siano (magari) nominati per cooptazione da parte degli stessi ordini dei giornalisti e del mondo accademico del diritto, secondo un modello di alternanza di tipo turnario.

L'istituzione di tale autorità, inoltre, sarebbe del tutto in linea col disegno europeo del DSA e del DMA. Infatti, così come l'Unione europea si è riappropriata della potestà regolamentatrice in materia di mercato e servizi digitali, allo stesso modo l'autorità pubblica deve riappropriarsi della potestà giudicante in tema di servizi digitali, in quanto il potere di legiferare senza la capacità di offrire concreta tutela rischia di rimanere un potere monco.

Certo è, poi, che un tale garante deve comunque essere indipendente dalla politica, onde evitare quelle ingerenze sull'informazione tipiche dei regimi autoritari, perché l'informazione *corretta* dal potere politico corre il grave rischio di risultare "politicamente corrotta", nel senso che risentirebbe degli stessi vizi della martellante propaganda delle dittature. È opportuno, pertanto, che la nomina dei membri della prospettata autorità e i confini della sua azione non siano determinate dai governi nazionali, in quanto la libertà di informazione non può (e non deve) risentire delle scelte politiche della fazione che detiene il potere, ma deve favorire il dibattito tra istituzioni e garantire il diritto di espressione delle minoranze.

Quanto alle modalità di effettuazione del controllo sulla veridicità delle notizie, poi, un procedimento equo potrebbe essere quello del metodo a doppio cieco utilizzato in campo scientifico, seppure effettuato *ex post*. In questo modo, infatti, la fase di controllo del contenuto di un post verrebbe spogliata dal possibile pregiudizio sull'autore e sul modo di leggere i fatti riportati. Nello scenario delineato, quindi, ai social network verrebbe sottratto il compito di controllare direttamente i contenuti e restituita loro la vera natura di soggetti neutrali.

Tuttavia, ad essi rimarrebbe comunque il compito di disciplinare le modalità esecutive di sospensione, limitazione della visibilità, rimozione e ripristino dei contenuti segnalati e verificati dal garante[118], con l'esposizione a possibili reclami. Per la risoluzione di questa problematica, allora, è necessario che alla stessa autorità garante venga affiancato un organismo di mediazione che dirima *pro bono pacis* le controversie che potrebbero insorgere sulle rimozioni non valutate dal garante e che limiti l'incremento del contenzioso presso gli organi giudiziari (come del resto proposto anche dal DSA).

5. Una postilla conclusiva

In conclusione, le prospettate integrazioni potrebbero migliorare il quadro prefigurato dalle ultime proposte di regolamento europeo agendo a livello normativo e giudicante su tre distinti livelli.

Il primo di essi, sulla scia dell'acquisita sovranità da parte dell'UE in materia di mercato e servizi digitali, dovrebbe integrare le tutele del cittadino-utente-consumatore tramite un apposito *Statuto dei diritti e doveri sul Web* con lo scopo di uniformare e garantire i diritti del singolo all'interno dei confini dell'Unione. Tale documento, inoltre, dovrebbe contenere tutti quei principi fondamentali che vanno posti alla base della tutela civile e amministrativa approntata dagli Stati, riparando il cittadino dagli abusi delle multinazionali. Tra questi, andrebbe sancito una volta per tutte il divieto di censura privata e di sottoposizione a giudizio di "tribunali privati", come quello istituito nel Metaverso di Mark Zuckerberg (l'*Oversight Board*)[119].

Il secondo livello, invece, dovrebbe incidere sulle discipline statali depenalizzando (ove possibile) le condotte in argomento o differenziandone maggiormente la disciplina a cui andrebbe affiancata una cooperazione tra gli Stati per armonizzare le diverse discipline e risposte punitive nazionali, al fine di stabilire un livello primario di tutela del singolo e della collettività. Andrebbero disciplinati in questo livello, inoltre, tutti quegli aspetti della vicenda contrattuale nei servizi digitali (sottoscrizione delle condizioni generali, recesso unilaterale della parte dominante, etc.), che non possono più rimanere sforniti di specifica tutela positiva.

Il terzo livello, infine, deve incidere sulle discipline di *soft law* tramite l'eliminazione delle deleghe ai privati e la loro sostituzione con la *contrattualizzazione* in senso collettivo delle autoregolamentazioni (tramite un confronto *multi-stakeholder* sul modello brasiliano), volta a limitare ulteriormente l'eccessivo potere acquisito dalle multinazionali negli ultimi decenni.

A presidio dei tre livelli prospettati, poi, vanno poste tutte le autorità (giudici, garanti, mediatori) che possono tutelare la parte debole dei rapporti sul Web con le stesse modalità con cui vengono tutelate le parti deboli di altri rapporti (*ex multis*, lavoratori, consumatori, subfornitori, contribuenti e così via).

Note

[1]Per un approfondimento del tema dal punto di vista sociologico si veda E. Mangone, *Incertezza, Futuro, Narrazione*, NaSC Free Press, 2021; più sintetico M. Sorice, *La partecipazione politica nel tempo della post-democrazia*, in "Culture e Studi del Sociale-CuSSoc", 2020, n. 2; dal punto di vista filosofico e biogiuridico A.R. Vitale, *All'ombra del covid-19. Guida critica e biogiuridica alla tragedia della pandemia*, Il Cerchio editore, 2022.

[2]Da più parti è stata segnalata l'importanza di una regolamentazione dei sistemi di controllo dell'informazione sul Web e sui pericoli che possono derivare da un'azione non adeguatamente lucida nelle premesse. Appare evidente, ormai, che la gestione della rete ha importanti ricadute sulla libertà di espressione (cfr. *ex multis* G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in "MediaLaws", 2018, n. 1; cfr. anche P. Dunn, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech*, in questa Rivista, 2022, n. 1), ma ha rilevanti ricadute anche sul piano della difesa e della sicurezza nazionale, come osservato anche dall'istituto del *CFIUS* e riportato in G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma*, *ivi*.

[3]Appare interessante sul punto quanto osservato da Michele Sorice sul conflitto tra i vecchi spazi pubblici della società di massa e la nuova *network society* che, lungi dall'essere egualitaria tende a legittimare un «pensiero unico» (cfr. M. Sorice, *La partecipazione politica nel tempo della post-democrazia*, cit.). Anche la dottrina costituzionalistica ha osservato che la questione sulla polarizzazione del pensiero impedisce il dibattito democratico, trasformando i toni critici del confronto in aspra polemica (cfr. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., p. 10); non meno autorevoli, poi, sono le critiche all'ampio uso di algoritmi per distribuire l'informazione. La dottrina è vastissima, ma basti segnalare quanto osservato in A.C. Amato Mangiameli, *Intelligenza artificiale, big data e nuovi diritti*, in questa Rivista, 2022, n. 1, §§ 5-7.

[4]Il sistema costruito sulla Direttiva 2000/31/CE è stato, invero, oggetto di recenti modifiche di cui si parla nel testo.

[5]In tal senso, si ponga attenzione anche a impianti normativi di *soft law* come quello del *Code of Practice on Disinformation* con il quale è stato delegato alle *big tech* il compito di regolamentare il fenomeno della disinformazione con linee generali interne (cfr. doc. COM(2018) 236 final del 26 aprile 2018, § 3.1.4). Sul punto è stato evidenziato che il quadro normativo entro cui si muove il Codice «non è esente da elementi di contraddizione, specie per l'attenzione "eccezionalista" con cui le politiche europee sembrano guardare alla informazione online» (così C. Magnani, *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in "Forum di quaderni costituzionali", 4 aprile 2019, p. 11); in linea con tale osservazione la tesi per cui il Codice ha posto le basi per una censura privata (*ex multis* M. Monti, *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", 24 aprile 2020, §§ 4-5; cfr. anche Id., *"Censura privata", così si incrina il modello delle big tech*, in "Agenda Digitale", 26 giugno 2020). Sul profilo dell'efficacia, poi, è stato ritenuto che il *soft law* ha il limite si essere una fonte debole dalla capacità coercitiva discutibile (così P. Bonini, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in "Federalismi.it", 24 aprile 2020, p. 268).

[6]Oggi si assiste, infatti, alla creazione di un doppio livello di disciplina che vede da una parte l'impegno diretto degli Stati e dall'altra l'impegno delle singole piattaforme nel formulare molteplici discipline per fronteggiare i fenomeni illeciti diffusi sul Web.

[7]Importantissimo sul tema della fondamentale importanza dell'accesso a Internet S. Rodotà, *Nota di Stefano Rodotà per le audizioni sui disegni di legge sull'accesso a Internet presso la Commissione Affari costituzionali del Senato*, in "www.senato.it", p. 4; sul tema meritano menzione anche Id., *Una costituzione per Internet*, in "Politica del diritto", 2010, n. 3, p. 351; C. Caruso, *L'individuo nella rete: i diritti della persona al tempo di internet*, in "Forum di quaderni costituzionali", 28 aprile 2013; P. Passaglia, *Diritto di accesso ad Internet e giustizia costituzionale. Una preliminare indagine comparata*, in "Consulta Online", 2011.

[8]In proposito, tra tanti, merita attenzione l'analisi di Scorza, il quale nitidamente ha osservato che si è pericolosamente lasciato che le big five si appropriassero di poteri di esclusivo appannaggio dello Stato (cfr. G. Scorza, *In principio era Internet e lo immaginavamo diverso*, in questa Rivista, 2022, n. 1, pp. 2-3).

[9]Sul tema è stato sostenuto che le agenzie di *fact-checking* sono legate ad ambienti che ne minano l'imparzialità, rendendo necessario un controllo pubblico (così M. Monti, *Fake news e social network: la verità ai tempi di Facebook*, in "MediaLaws", 2017, n. 1, p. 88); inoltre, cfr. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., §§ 5-6, il quale avverte che l'uso di algoritmi potrebbe far rinchiudere un soggetto all'interno di una *bolla*, minando il pluralismo democratico; sul punto si è detto anche che le gli algoritmi «permettono alle piattaforme digitali di influenzare le scelte (anche politiche) dei propri utenti e di coartarne in qualche modo la volontà» (così M.R. Allegri, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in questa Rivista, 2021, n. 2, p. 11.

[10]Per una completa disamina delle teorie sulla qualifica del rapporto tra società operanti su piattaforme digitali e utente, un contributo assai esaustivo è R. Cosio, *Facebook e Social. Natura del contratto tra utente e social*, in "Ricerche giuridiche", vol. 6, 2017, n. 1, con particolare riferimento ai §§ 3-5.

[11]È stato evidenziato in dottrina che esiste «un potere estremo nel decidere chi deve stare zitto e chi non deve più essere ascoltato», denunciando che i social media hanno la possibilità di influenzare il dibattito tramite la privatizzazione della censura (così G.L. Conti, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, in "Rivista AIC", 2018, n. 4, pp. 209-216); sul tema cfr. anche M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in questa Rivista, 2019, n. 1, p. 38; G. Pitruzzella, *Il web ha bisogno di regole non di «censura privata»*, in "Corriere della Sera", 8 novembre 2019; A. Venanzoni, M. Monti, *Il tramonto della frontiera digitale? Note a prima lettura dell'executive order del 28 maggio 2020 emanato per prevenire la censura online da parte dei social media*, in "Diritti Comparati", 8 giugno 2020.

[12]Cfr. Trib. di Roma, sez. spec. in materia di impresa, ord. 11 dicembre 2019; Trib. di Roma, sez. civ. XVII, ord. 29 aprile 2020. Sulla prima delle due è sorto anche un dibattito in dottrina di cui si riportano, *ex multis*, C. Caruso, *La libertà di espressione presa sul serio. Casa Pound c. Facebook, atto I*, in "SIDIBlog", 20 gennaio 2020; P. De Sena, M. Castellaneta, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, *ivi*, 20 gennaio 2020.

[13]Cfr. Trib. di Roma, ord. 11 dicembre 2019, cit., p. 4.

[14]Non si trascuri, inoltre, che le stesse imprese proprietarie delle piattaforme digitali affidano i controlli sul rispetto delle loro linee guida ad algoritmi che sovente demonetizzano, deindicizzano o censurano contenuti che l'ordinamento non ritiene affatto dannosi. Così, allora, ci si è interrogati sull'effettiva funzionalità degli algoritmi che censurano nudi artistici, spettacoli comici che usano turpiloquio o battute ritenute lesive della dignità di talune categorie, mentre non riescono a tutelare gli utenti da forme di aggressività o prevaricazione nascosta da un linguaggio elegante.

[15]Cfr. Trib. Roma, sez. diritti della persona e immigrazione civile, ord. 23 febbraio 2019.

[16]*Ex multis*, C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in "Consulta Online", *Liber Amicorum per Pasquale Costanzo*, 17 marzo 2020. Va, però, segnalato che altra parte della dottrina, in senso opposto (e forse più affine all'ordinanza del 23 febbraio 2019), ha sostenuto che l'importanza assunta dai social network non li rende indispensabili per la manifestazione del pensiero (cfr. M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in questa Rivista, 2021, n. 2, p. 55).

[17]«L'impianto argomentativo dell'ordinanza [...] non persuade. È arduo desumere un obbligo di rimozione da discipline tra loro assai diverse per forza, rango ed ambito di applicazione» (C. Caruso,*I custodi di silicio*, cit., § 4).

[18]*Ex multis*, C. Cost. nn. 348/2007, 349/2007, 49/2015.

[19]Anche la dottrina che pare aderire al secondo filone giurisprudenziale, invero, sembra contraria a riconoscere un potere di controllo (e conseguenti responsabilità) ai social network, in quanto ciò li assimilerebbe agli editori (emancipazione di cui neanche il DSA è portatore), cfr. M. Bassini, *Libertà di espressione e social network*, cit., p. 56.

[20]La scelta di aderire al primo orientamento è influenzata anche dalla giurisprudenza costituzionale tedesca del 2019, la quale ha sostenuto che Facebook costituisce ormai uno spazio importante per la garanzia del principio pluralistico (cfr. M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in "MediaLaws", 2021, n. 1, p. 93).

[21]*Ex multis*, per i limiti al diritto di cronaca, cfr. Cass. pen., sez. V, 14 settembre 2016 n. 42987; per i presupposti e il perimetro applicativo del diritto di critica il diritto di critica nella diffamazione su Facebook, cfr. Cass. pen., sez. I, 20 agosto 2014 n. 36045.

[22]Si riporta che anche secondo il Comunicato stampa del 13 maggio 2021 dell'AGCM si attesta che «Google detiene una posizione dominante che le consente di controllare l'accesso degli sviluppatori di app agli utenti finali. [...] è un operatore di assoluto rilievo, a livello globale, nel contesto della cosiddetta economia digitale e possiede una forza finanziaria rilevantissima».

[23]Sul tema cfr., *ex multis*, O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in "Consulta Online", 10 febbraio 2014, p. 27, il quale osserva che, sebbene l'attività degli ISP si avvicina effettivamente a quella editoriale, non bisognerebbe inquadrare tale attività nell'ambito di un controllo sui contenuti.

[24]Va segnalato che, in Europa, un simile caso avrebbe certamente comportato rilevanti conseguenze sul piano sanzionatorio Amazon e Google, anche alla luce dell'art. 102 TFUE, il quale vieta lo sfruttamento di posizioni dominanti sul mercato interno o su una parte sostanziale di questo.

[25]A tal proposito è stato osservato che il DMA innova la disciplina *antitrust*, anticipando la tutela dalle condotte abusive dei *gatekeeper* (cfr. N. Giusti, *Digital Markets Act (DMA), c'è l'accordo tra Consiglio e Parlamento UE: le nuove regole*, in "CyberSecurity 360", 28 marzo 2022).

[26]Cfr. M.R. Allegri, *Il futuro digitale dell'Unione europea*, cit., pp. 11-12.

[27]Cfr. B. Calderini, *Digital Markets Act, perché le Big Tech temono il piano Ue*, in "Agenda Digitale", 7 aprile 2022; v. anche T. Madiega, *Regulating digital gatekeepers. Background on the future Digital Markets Act*, European Parliamentary Research Service, December 2020, p. 9.

[28]*Ex multis*, cfr. S. Stolton, *EU negotiators agree new rules to rein in tech giants. 'The Digital Markets Act puts an end to the ever-increasing dominance of Big Tech companies,' says lead MEP*, in "Politico", 24 March 2022; il medesimo entusiasmo pare trasparire anche dal Comunicato stampa del Parlamento europeo del 23 novembre 2021.

[29]Tali fatti, invero, sono tutti riconducibili al fenomeno della polarizzazione del dibattito nei social network, spesso condizionato dagli algoritmi che veicolano le campagne di marketing. Sul tema è stato sostenuto che su Internet «persone della stessa area ideologica, al termine di una discussione fra loro, finiranno per pensare la stessa cosa che pensavano prima, ma in forma più estremistica» perché l'esposizione ripetuta a una posizione estrema le porterà a credervi (cfr. C.R. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?*, il Mulino, 2003, pp. 82-87; è rilevato anche che i social network sono costruiti con algoritmi che connettono tra loro persone della stessa nicchia, esponendole a un'unica versione, formando *bolle* o *echo-chambers* (così G. Ruffo, M. Tambuscio, *Capire la diffusione della disinformazione e come contrastarla*, in "Federalismi.it", 24 aprile 2020, pp. 74-75.

[30]*Ex multis*, G. Calvani, *Battaglione Azov su Facebook, cos'è e perché è permesso elogiarlo*, in "Ultima Voce", 5 marzo 2022.

[31]Cfr. Rete nazionale per il contrasto ai discorsi e ai fenomeni d'odio, *Meta consente incitamento all'odio: un (altro) pessimo segnale*, in "Amnesty International Italia", 14 marzo 2022.

[32]Cfr., *ex multis*, M. D'Alessandro, *Il caso del corso di Paolo Nori su Dostoevskij all'università Bicocca*, in "AGI-Agenzia Italia", 2 marzo 2022; C. Ribichini, *Il sindaco Sala: "Escludo Gergiev sul podio della Scala il 5 marzo"*, in "SkyTG24", 28 febbraio 2022; L. Rao, *TikTok ha sospeso il caricamento di video in Russia*, in "Fanpage.it", 7 marzo 2022; K. Carboni, *La guerra dei social contro Putin e la guerra di Putin contro i social*, in "Wired", 26 febbraio 2022.

[33]«Cittadini più maturi [...] hanno bisogno di un percorso educativo nuovo [...] in quanto la potenza e la pervasività degli strumenti e dei paradigmi del digitale richiedono un salto di qualità [...] Ciò significa soprattutto riconoscere gli altri, ancora prima delle loro idee [...] non aver paura di confrontarsi; avere il coraggio di riconoscere i propri errori e cambiare idea», così V. Azzollini, *Chi ha paura della libertà di internet?*, in "IBL, 13 dicembre 2019.

[34]Sulla descrizione del percorso degenerativo del fenomeno cfr. D. Palano, *La bolla mortale della nuova democrazia*, in "Il Foglio", 28 aprile 2017; più approfondito Id., *Bubble Democracy. La fine del pubblico e la nuova polarizzazione*, Scholè editore, 2020; parimenti approfondito anche Id., *La democrazia alla fine del «pubblico». Sfiducia, frammentazione, polarizzazione: verso una «bubble democracy»?*, in "Governare la paura", 2019, aprile, p. 35 ss.; cfr. anche G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., §§ 5, 6, 8, 14.

[35]Cfr. a tal proposito Commissione europea, *The Digital Services Act package*.

[36]«"L'accordo sul Dsa è storico" [...] obbliga le Big Tech ad assumere maggiore responsabilità sui contenuti illegali o nocivi che circolano sulle loro piattaforme», R. Bucca, M. Sabatini, *Digital Services Act, la Ue a una svolta: cosa cambia per utenti, aziende e big tech*, in "Agenda Digitale", 19 maggio 2022.

[37]Cfr. M.R. Allegri, *Il futuro digitale dell'Unione europea*, cit., § 4; G.M. Ruotolo, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in questa Rivista, 2022, n. 1 § 2. Si segnalano alcune voci critiche sui possibili attriti tra normative UE, cfr. C. Morelli, *L'Unione Europea e i Digital Acts. Lo studio commissionato dalla commissione parlamentare speciale sull'Intelligenza artificiale AIDA: al via la discussione sulla bozza di regolamento AI Act*, in "Altalex", 7 febbraio 2022; criticità anche sul profilo attuativo, cfr. N. Giusti, A. Longo, *Digital services act: molti vantaggi per utenti ed Europa, ma sarà una sfida attuare le nuove norme*, in "CyberSecurity 360", 24 aprile 2022; F.M.R. Livelli, *Digital Services Act, cos'è, cosa prevede, perché rischia di essere una tigre di carta*, in "Risk Management 360", 4 maggio 2022.

[38]Questa è una delle perplessità espresse in dottrina anche sulla legislazione tedesca.

[39]Cfr. la norma citata con gli artt. 3 della legge 7 agosto 1990 n. 241, e 7 del d.l. 27 luglio 2000 n. 212.

[40]Consultabile sul sito di Légifrance.

[41]Per un'analisi più approfondita si consiglia la lettura di T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in "Discrimen", 15 giugno 2020, pp. 20-23.

[42]Le maggiori critiche del principale sindacato dei giornalisti francesi ha riguardato la circostanza che il giudice decide

sulla rimozione entro 48 ore, lamentandone la «visione liberticida», ma con la *Décision n. 2018-773 DC* del *Conseil constitutionnel* è stata dichiarata la legittimità della norma (cfr. T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, 2020, pp. 88-89; cfr. anche Id., *La tutela penale della libertà*, cit., pp. 22-23).

[43]Per la versione italiana della normativa v. G. Giannone Codiglione, *Legge per migliorare la tutela dei diritti sui social network (Netzwerkdurchsetzungsgesetz – NetzDG)*, in "MediaLaws", 2017, n. 1, pp. 185-190; un'analisi dei contenuti della legge è contenuta anche in A. Kapeller, *La legge contro gli abusi sui social networks in Germania*, in "Altalex", 7 marzo 2018; cfr. anche M. Fiorillo, *Fake news sul web: il drastico intervento della Germania*, in "Inside Marketing", 16 ottobre 2017.

[44]Per una disamina più approfondita v. T. Guerini, *La tutela penale della libertà*, cit., pp. 24-27.

[45]L'entità delle sanzioni aggrava il dubbio di chi ritiene che i social network, per evitarle, potrebbero eccedere di "zelo censorio", anche perché non è prevista una sanzione per la rimozione ingiustificata di contenuti leciti (in tal senso C. Magnani, *Libertà d'informazione online e fake news: vera emergenza?*, cit., p. 16); negli stessi termini T. Guerini, *La tutela penale della libertà*, cit.; cfr. anche V. Claussen, *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, in "MediaLaws", 2018, n. 3, p. 122; è stato segnalato anche il rischio che i social network «finiscano per consentire solo la diffusione di contenuti mainstream [...] rimuovendo in automatico qualsiasi contenuto che abbia suscitato [...] una contestazione» (così A. Mazziotti di Celso, *Dal Primo Emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali*, in "MediaLaws", 2018, n. 3, p. 107).

[46]Cfr. *Democracy Index 2021*, in "Economist Intelligent - EIU", 10 February 2022.

[47]Per dar conto delle dovute differenze, si rimanda integralmente alla disamina contenuta in O. Pollicino, *Fundamental Rights as Bycatch – Russia's Anti-Fake News Legislation*, in "Verfassungs Blog", 28 marzo 2019, § 3. L'autore, invero, manifesta parecchie perplessità sul regime normativo della novella del 2019, riportando anche il contrasto con la CEDU e con la stessa giurisprudenza costituzionale russa sui principi di proporzione e di certezza del diritto. Altra voce critica della riforma del 2019 è Ilmira Galimova, la quale lamenta tanto l'estensione del concetto di "luogo pubblico" sull'ambito della rete, quanto le lacune sul meccanismo di filtraggio riservato al Procuratore generale (cfr. I. Galimova, *La Duma introduce nuove restrizioni alla rete*, in "Nomos", 2019, n. 1).

[48]Il meccanismo pare simile alla previsione del DSA sulla responsabilità delle piattaforme che acquisiscono la conoscenza dell'illiceità di un contenuto.

[49]Cfr. il testo novellato dell'art. 15-3 Legge Federale n. 149-FZ.

[50]Cfr. Legge Federale n. 32-FZ del 4 marzo 2022 nel testo originale.

[51]Invero, ciò che veramente lascia una macchia sull'esperienza giuridica russa è la sostanziale dipendenza degli organi di controllo dal governo federale, in quanto ciò ne vizia la terzietà e l'indipendenza reali.

[52]Invero, il giudizio sull'apprezzabilità di un sistema giuridico va tenuto distinto dal giudizio sul modello politico di una Nazione. Va, difatti, rammentato che anche in Italia sopravvivono importanti codificazioni e innumerevoli sistemi burocratici del ventennio fascista, che spesso sono stati ritenuti legittimi anche in sede di vaglio di costituzionalità. Ci si permette di sostenere, quindi, che il vero problema della Federazione Russa è di tipo culturale e politico, e non di mera compilazione normativa.

[53]Cfr. I. Galimova, *La Duma introduce nuove restrizioni alla rete*, cit., p. 5.

[54]Cfr. F. Spidalieri, F. Voce, *Cybersecurity, America Is back? La nuova politica Usa, dagli slogan ai fatti*, in "Agenda Digitale", 14 settembre 2021. Invero, anche in Italia è stato autorevolmente notato che la tutela delle informazioni in rete ha un rilievo strategico e di sicurezza rilevanti: *ex multis*, cfr. A. Di Corinto, *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in questa Rivista, 2022, n. 1).

[55]Cfr. M.A. Cutrufo, *Tutti i pericoli di TikTok, il nuovo social che spaventa gli USA*, in "Agenda Digitale", 9 dicembre 2019; A. Di Corinto, *L'app lgbt Grindr torna in mano Usa, troppo pericoloso lasciarla ai cinesi*, in "La Repubblica", 17 maggio 2019; P. De Luca, *I nuovi regolamenti del CFIUS*, in "Geopolitica.info", 22 gennaio 2020; G. Di Donfrancesco, *Dazi, cybersecurity, finanza: tutte le guerre di mercato Usa-Cina*, in "Il Sole24Ore", 17 febbraio 2018.

[56]*Ex multis*, A. Mallamaci, *Gli Usa creano il "Comitato per la governance della disinformazione": cos'è e perché fa discutere*, in "Agenda Digitale", 4 maggio 2022, che riporta i timori sull'iniziativa e paventa la nascita di un "Ministero della Verità" di orwelliana memoria. La critica, invero, riprende un'opinione espressa più di un decennio fa in una sentenza della stessa Corte Suprema degli Stati Uniti in cui si affermava (in merito alla legittimità costituzionale dello *Stolen Valor Act*) che «Our constitutional tradition stands against the idea that we need Oceania's Ministry of Truth» (caso *Stati uniti vs. Alvarez*, ottobre 2011, p. 15).

[57]Cfr. T. Lorenz, *How the Biden administration let right-wing attacks derail its disinformation efforts*, in "The Washington Post", 18 May 2022; A. Mallamaci, *Gli Usa creano il "Comitato per la governance della disinformazione"*, cit., in cui si riporta anche il timore degli statunitensi di subire forme di sorveglianza governativa. Si dà riscontro, poi, del fatto che anche nella Scheda informativa, resa nota il 2 maggio 2022, non sono esplicitati chiaramente gli scopi dell'istituzione.

[58]Si è rilevato che a richiedere le maggiori limitazioni della libertà sono gli "esponenti del mondo liberale e progressista", che invocano l'introduzione di «strumenti di controllo [...] che stridono con alcuni capisaldi della [...] libertà di espressione» (così A. Mazziotti di Celso, *Dal Primo Emendamento al bavaglio malese*, cit., p. 106).

[59]*Ivi*, pp. 107-108.

[60]Cfr. soprattutto *infra* § 4.3.

[61]Si pensi al delitto di diffamazione, all'ingiuria o alla lettura estensiva dell'art. 2059 c.c. in tema di privacy.

[62]Tra i più rilevanti cfr. artt. 612-*ter*, 615-*ter*-615-*quinquies*, 617-*quater*-617-*sexies*, 635-*bis*, 640-*ter* c.p., nonché i riferimenti contenuti in diverse leggi speciali (*ex multis* d.lgs. 8 giugno 2001, n. 231).

[63]*Ex multis*, artt. 270-*quinquies*, co. 2, 544-*quinquies*, co. 2, n. 2, 609-*duodecies* c.p.

[64]La giurisprudenza ritiene che «nulla rileva, ai fini della sua esclusione, il fatto che non si sia verificato alcun turbamento dell'ordine pubblico, essendo sufficiente che vi fosse un'astratta possibilità che un tale turbamento in effetti si verificasse» (così Cass. pen., sez. I, 7 novembre 1996 n. 9475).

[65]Ovvero a seguito della deliberazione di cui all'art. 78 Cost.

[66]Anche solo estendendo il principio espresso in Cass. pen., sez. V, 14 novembre 2016 n. 4873.

[67]Cfr. C. Guarnieri, *Social media e manipolazione dell'opinione pubblica*, in "Amnesty international Italia", 29 maggio 2017; E. Menietti, *Il caso Cambridge Analytica*, in "Il Post", 19 marzo 2018; D. Marino, *Social media e manipolazione di massa, le leggi sono rotte: come salvare la democrazia?*, in "Agenda Digitale", 29 maggio 2019.

[68]Sul tema cfr. G. Matucci, *Informazione online e dovere di solidarietà. Le fake news fra educazione e responsabilità*, in "Rivista AIC", 2018, n. 1.

[69]Cfr. quanto osservato sulla propagazione di fake news grazie alla spinta alla condivisione in G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., p. 12.

[70]Uno studio pubblicato dall'AGCOM ha rilevato che solo una piccola parte della popolazione (il 2%) è capace di distinguere sempre le notizie vere da quelle false (AGCOM, *Percezione e disinformazione. Molto "razionali" o troppo "pigri"?*, febbraio 2020, pp. 35-36). Già da anni, inoltre, si propone di andare oltre il semplice utilizzo dell'espressione fake news, che non descrive la complessità dei fenomeni della misinformazione (l'involontaria condivisione di informazioni false) e della disinformazione (la deliberata creazione e condivisione di informazioni note per essere false). Sul punto cfr. C. Wardle, *Fake news. It's complicated*, in "First draft", 16 February 2017; in tema di distinzione tra disinformazione, errore non intenzionale, "rumori", teorie cospirative, satira, false affermazioni di politici, report che possono ingannare e opinioni cfr. il più volte citato articolo di Pitruzzella (G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., § 9).

[71]«Con l'intenzione di collocare le fake news in un territorio sicuramente distinto rispetto a quello delle opinioni e dei valori [...] hanno dato la seguente definizione [...]: sono quegli articoli recanti notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno i lettori» (G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., pp. 13-14). Va, peraltro, precisato che il *Code of Practice on Disinformation* espressamente dispone che «The notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary, and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising» (cfr. *EU Code of Practice on Disinformation*, p. 1).

[72]Per l'analisi testuale si rinvia agli originali disegno di legge 7 febbraio 2017, n. 2688 (c.d. *ddl Gambaro*) e disegno di legge 14 dicembre 2017 n. 3001 (c.d. *ddl Zanda-Filippin*).

[73]Cfr. M. Monti, *La XVII legislatura e la libertà di espressione: un bilancio fra luci e ombre*, in "Osservatorio sulle fonti", 2018, n. 2, p. 17-18; M. Monti, *La proposta del ddl Zanda-Filippin sul contrasto alle fake news sui social network: profili problematici*, in "Diritti Comparati", 7 dicembre 2017, p. 6.

[74]Cfr., *ex multis*, M. Fumo, *Bufale elettroniche, repressione penale e democrazia*, in "MediaLaws", 2018, n. 1, p. 83 ss.; C. Melzi d'Eril, *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, *ivi*, 2017, n. 1; M. Cuniberti, *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, *ivi*, 2017, n. 1, p. 30.

[75]In tal senso, E. Lehner, *Fake news e democrazia*, in "MediaLaws", 2019, n. 1, p. 8.

[76]Cfr. art. 1, co. 3, ddl n. 2688/2017. Sul punto, inoltre, è stato correttamente osservato (e motivato) che l'esclusione della punibilità del giornalismo professionale contraddice gli scopi della normativa e ne distorce il senso (cfr. C. Melzi d'Eril, *Fake news e responsabilità*, cit., p. 62); tuttavia, va rilevato che c'è chi ritiene che un'assimilazione *tout court* tra social network e editori potrebbe essere di detrimento per il pluralismo, data l'importante funzione svolta da questi ultimi (cfr. O. Pollicino, *Tutela del pluralismo nell'era digitale*, cit., p. 27).

[77]Infatti, il professionista e l'utente sono parimenti esposti al pericolo di avere percezioni errate, fuori dal giudizio critico (i c.d. *bias* cognitivi), seppur in buona fede e nell'inconsapevolezza del fenomeno. Sarebbe opportuno, quindi, non esitare nell'ammettere che nessuno è esente dal rischio di immettere nel mercato dell'informazione una notizia falsa.

[78]Di opinione affine B. Saetta, *Per una regolamentazione delle piattaforme digitali*, in "Valigiablu", 8 novembre 2019; critici sul tema della censura privata V. Azzollini, *Chi ha paura della libertà di internet?*, cit. e O. Grandinetti, *Le piattaforme digitali come "poteri privati" e la censura online*, in questa Rivista, 2022, n. 1.

[79]Cfr. P. Bonini, *L'autoregolamentazione*, cit., p. 281.

[80]Già nel 2018 la Commissione europea esprimeva la stessa preoccupazione (cfr. doc. COM(2018) 236 final del 26 aprile 2018), condivisa anche negli USA (cfr. G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale*, cit.; H. Allcott, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, in "Journal of Economic Perspectives", vol. 31, 2017, n. 2).

[81]V. *supra* § 2.2; cfr. anche M.R. Allegri, *Il futuro digitale dell'Unione europea*, cit., pp. 11-12; V. Bertola, *La sovranità digitale e il futuro di Internet*, in questa Rivista, 2022, n. 1.

[82]Che pare essere la strada intrapresa da ultimo anche dal legislatore europeo. Si evidenzia, poi, che la dottrina rileva l'esigenza di creare un'apposita "Carta dei diritti" (*ex multis*, cfr. A.C. Amato Mangiameli, *Intelligenza artificiale, big data e nuovi diritti*, cit., § 7 e relativi riferimenti bibliografici); sul tema della cooperazione cfr. J. Ciani Sciolla, *Diritto all'oblio e cooperazione internazionale: problemi e prospettive*, in questa Rivista, 2022, n. 1, § 1, seppure l'Autore si riferisca principalmente al diritto all'oblio.

[83]Si tratta dell'eterno confronto tra libertà e sicurezza, sul quale merita speciale menzione la riflessione del Vicepresidente dell'Autorità garante per la privacy, la quale correttamente sostiene che tale rapporto non può essere ricostruito come conflitto, o si rischia di sacrificare valori importantissimi per una democrazia (cfr. G. Cerrina Feroni, *Sicurezza e diritti, la tutela della libertà nel "permanente stato d'eccezione"*, 17 dicembre 2020).

[84]A tal riguardo si pensi al fatto che se il *Code of Practice on Disinformation* fosse stato agganciato ad una disciplina similare a quella del DSA forse non sarebbero nati quei centri di potere che hanno reso le *big five* le "signore della verità e della censura". Sul tema si noti che quanto notato sul ruolo della *governance* di Internet e della sua capacità di influenzare la società in D. Getschko, C. Afonso, A.F. Barbosa, *Il ruolo della governance multi-stakeholder di Internet nella diffusione della connettività in Brasile*, in questa Rivista, 2022, n. 1.

[85]Cfr. il termine *Fatto*, in "Definizioni, etimologia e citazioni", Treccani.

[86]Cfr. il termine *Opinione*, *ivi*.

[87]Sul punto va rilevato che il diritto di critica online trova comunque il suo limite nel rispetto della normativa per il contrasto all'*hate speech*.

[88]Sul ruolo attuale e l'auspicio di una modifica degli algoritmi, cfr. G. Cassano, *L'ostracismo nell'era digitale. Il caso Trump, la cacciata dai social media ed il diritto positivo*, in "Penale. Diritto e Procedura", 5 marzo 2021, § 8; cfr. anche P. Stanzione, *Strapotere delle piattaforme, tutela contro l'algocrazia*, in "La Repubblica", 2 luglio 2021; M. Martorana, *Censura sui social network: come funziona, chi colpisce e perché*, in "Agenda Digitale", 14 ottobre 2021; S. Fiabane, V. Damiano, *La gestione dei contenuti nella società dell'algocrazia: il vero potere è nelle mani di chi gestisce gli algoritmi*, in "Agenda17", 26 novembre 2021; M. Cuniberti, *Potere e libertà nella rete*, in "MediaLaws", 2018, n. 3.

[89]Sul punto il DSA sembra prendere una posizione netta, ma va chiarito che, essendo ormai Internet uno spazio irrinunciabile per molte attività, esserne esclusi potrebbe essere paragonato a sanzioni come l'interdizione dal frequentare un luogo o (persino) l'esilio. Senza voler fare paragoni impropri, la limitazione di diritti fondamentali rischia di somigliare al feno-

meno che in campo penalistico viene definito con l'espressione "fine pena mai".

[90]In tal senso, la Raccomandazione CM/Rec(2014) 6 del Comitato dei Ministri del Consiglio d'Europa adottata il 16 aprile 2014, dispone già nelle sue prime righe l'assimilazione di Internet a un *servizio pubblico* cui è collegata la «legittima aspettativa di disporre di servizi online accessibili, forniti senza discriminazioni [...] sicuri, affidabili ed erogati con continuità» per l'esercizio «dei propri diritti umani e libertà fondamentali».

[91]Trib. di Roma, ord. 11 dicembre 2019, cit., p. 4.

[92]Non essendo più meramente contrattuale il rapporto tra utente e social network, appare opportuno che l'apparato para-sanzionatorio predisposto dal fornitore del servizio punti a permettere la riabilitazione del trasgressore per un suo "reinserimento nella società digitale".

[93]Si rifletta sul fatto per cui la piattaforma che esclude dal servizio un utente ne ha già acquisito i dati e ne ha estratto dei metadati (che risultano indistinguibili dopo la loro elaborazione) che continuerà a utilizzare per i suoi fini commerciali. Ciò comporta problemi sul piano del sinallagma, in quanto una parte non fruisce più di un servizio, mentre l'altra continuerà ad utilizzare i dati acquisiti in ragione del servizio. A questo punto ci sarebbe da chiedersi quali potrebbero essere anche i risvolti risarcitori di un'esclusione perpetua; sui temi di cui sopra, cfr. A. Soro, *I social network non sono gratuiti, i nostri dati sono il prezzo da pagare*, 14 ottobre 2013.

[94]Un approfondimento necessario sul tema in D. Marino, *Social media e manipolazione di massa*, cit.; tra le voci giornalistiche cfr., *ex multis*, R. Liguori, *Come i social possono influenzare il voto politico*, in "AGI-Agenzia Italia", 30 settembre 2019.

[95]Cfr. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., pp. 9-10.

[96]A. Andronico, *Governance*, in B. Montanari (a cura di), "Luoghi della filosofia del diritto", Giappichelli, 2009, pp. 259-262. Analoghe preoccupazioni sembrano emergere anche in G. Cerrina Feroni, *Libertà di espressione, Garante privacy: "Troppo potere alle big tech, ecco come intervenire"*, in "Agenda Digitale", 11 maggio 2021, in cui si sostiene persino che la pretesa di acquisire sempre più potere da parte delle piattaforme digitali rischia – oggi – di sfociare anche in pericolose forme di "privatizzazione della giustizia digitale su scala globale".

[97]P. Grossi, *L'Europa del diritto*, Laterza, 2010, pp. 254-255.

[98]M. Monti, *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news*, in "MediaLaws", 2019, n. 1, p. 323.

[99]Cfr. E. Grande, *I mobili confini della libertà di espressione negli Stati Uniti e il metro della paura*, in "Questione Giustizia", 2015, n. 4, § 2; S. Cedrola, *Hate speech: il confine tra la libertà di espressione e la censura*, in "Ius in Itinere", 1 giugno 2017, § 5; ma anche J. Rinceanu, *Verso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei social network*, in "Sistema Penale", 13 maggio 2022, pp. 21-22; M. Monti, *Guerra alle fake news, troppe deleghe a Facebook: a rischio il pluralismo informativo*, in "Agenda Digitale", 13 maggio 2020; Id., *Privatizzazione della censura e Internet platforms*, cit., p. 40.

[100]Cfr. M. Monti, *La disinformazione online*, cit., p. 301.

[101]Importante sul tema M. Bassini, *Libertà di espressione e social network*, cit., p. 56.

[102]Sul conflitto tra principi di diritto pubblico internazionale e regole applicate dall'*Oversight Board* (e le relative conseguenze) cfr. M. Donateo, A. Polimeni, *Facebook Oversight Board, che succede ora? Ecco perché può essere un'arma a doppio taglio*, in "Agenda Digitale", 11 febbraio 2021.

[103]Cfr. M. Fraundorfer, *Brazil's Organization of the NETmundial meeting: moving forward in global internet governance*, in "Global Governance", vol. 23, 2017, n. 3, p. 503 ss.; R. Echeberria, *Brazil needs to involve all stakeholders in Internet governance*, in "Internet Society", 14 August 2017.

[104]Già nell'esperienza della Repubblica di Weimar «Vi fu chi considerò il Consiglio come [...] una sorta di contropotere rispetto al parlamento e che [...] rappresentasse l'avvio di una democrazia organica» G. Gozzi, *Democrazia e pluralismo da Weimar alla Repubblica Federale Tedesca*, in "Scienza & Politica per una storia delle dottrine", vol. 2, 1992, n. 6, p. 88.

[105]Cfr. art. 2, co. 3, l. 10 ottobre 1990, n. 287.

[106]Cfr. F. Zamponi, *Diffamazione a mezzo social network e il rischio di collasso del sistema giustizia*, in "Diritto.it", 27 giugno 2019.

[107]Cfr. art. 5, co. 1 e 1-*bis*, d.lgs. 4 marzo 2010, n. 28.

[108]Sebbene sia escluso che i social network abbiano le responsabilità degli editori, è anche vero che il DSA pone un obbligo di controllo *ex post* dei contenuti pubblicati. In tal senso, allora, sarebbe opportuno che le società che gestiscono piattaforme digitali siano responsabili in solido con chi pubblica il contenuto illecito nel caso in cui decidano di non rimuoverlo o ne ritardino la rimozione.

[109]Cfr. *infra* § 4.3.

[110]Si pensi, ad esempio, al mancato guadagno del giornalista d'inchiesta che rivela un fatto controverso sul suo canale YouTube, dell'artista che pubblica un'opera dai contenuti espliciti su Instagram o del comico che adopera turpiloquio nella sua esibizione in *streaming*: queste figure – per quanto possano recare fastidio ad altri – stanno solamente esercitando un loro diritto e, pertanto, meritano riparo dalle rimozioni e demonetizzazioni illegittime dei propri contenuti.

[111]Si noti, tuttavia, che la disposizione di cui al par. 3 dell'art. 18 del DSA non risulta davvero dissuasiva per la piattaforma che dispone di ingenti capitali.

[112]Si è già rilevato sul punto che spesso l'utente è propenso ad entrare in una *bolla*, condividendo e leggendo solo informazioni che lo appagano.

[113]Che può dipendere da scarsa educazione nell'utilizzo della rete (cfr. AGCOM, *Rapporto sul consumo di informazione*, febbraio 2018; AGID, *Competenze digitali per i cittadini: proposte operative*, 11 marzo 2020), o dall'uso di messaggi sensazionalistici che sfruttano le emozioni dell'utente (cfr. V. Azzollini, *Chi ha paura della libertà di internet?*, cit., p. 8).

[114]Lo stesso *Code of Practice on Disinformation* pare tenere conto di questa distinzione ove afferma che «The notion of "Disinformation" does not include [...] reporting errors».

[115]Perplessità sono state mostrate tanto al controllo umano (M. Monti, *Fake news e social network*, cit., p. 88), quanto all'attività svolta da algoritmi (così G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in "MediaLaws", 2020, n. 1, p. 33; M. Monti, *Privatizzazione della censura e Internet platforms*, cit., pp. 38-39).

[116]L'idea di un Ente specializzato è stata criticata come latrice del "Tribunale della verità" da voci autorevoli (*ex multis* cfr. A. Soro, *Il giusto rimedio contro le fake news*, in "La Repubblica", 8 marzo 2017). Lo stesso Pitruzzella, inoltre, pur proponendola si dice "non affezionato" all'idea di istituire un'autorità specializzata (cfr. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., p. 26).

[117]La figura di un garante contro la disinformazione è stata ipotizzata tanto come autorità che collabora con i *fact-checkers* (così G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., p. 26), quanto come Autorità garante del digitale di rinforzo all'opera di altre autorità esistenti (Garante per la privacy, Garante della concorrenza e del mercato e AGCOM) per il corretto uso di Internet e la tutela del pluralismo e della trasparenza dell'informazione (cfr. D.

Marino, *Social media e manipolazione di massa*, cit.; cfr. anche S. Foà, *Pubblici poteri e contrasto alle fake news. Verso l'effettività dei diritti aletici?*, in "Federalismi.it", 24 aprile 2020, p. 264).

[118]Così sarebbero superati anche i limiti della legge tedesca, in quanto i social network dovrebbero attivarsi solo per segnalare la presenza di contenuti di dubbia liceità all'autorità garante (sospendendone momentaneamente la visibilità), ed eseguirne la cancellazione o il ripristino dopo la sua pronuncia.

[119]L'istituzione dell'*Oversight Board* rischia di far riaffiorare le preoccupazioni palesate da Andronico (cfr. § 4.1.1.), in quanto sembra riprendere l'idea dell'appropriazione delle prerogative giudicanti presenti nelle Signorie medievali, strappando illegittimamente dalle mani dello Stato uno dei tre poteri che la cultura filosofico-giuridica della modernità gli ha affidato. In merito al funzionamento dell'organismo, poi, va rilevato che non sembra neanche aderire ai valori di tutela del singolo e certezza del diritto. Infatti, lo stesso procedimento di decisione è anomalo, in quanto – a fronte del brevissimo termine perentorio entro cui l'utente può proporre ricorso (15 giorni) – non vi è alcuna certezza sul *se* e sul *quando* una decisione verrà presa, perché «l'Oversight Board stabilisce quali casi verranno esaminati» (cfr. *Procedura di ricorso*, § 02). Non si trascuri, infine, che l'organismo non può essere considerato nemmeno come arbitro, in quanto assume decisioni su diritti indisponibili, in violazione dell'art. 806, co. 1, c.p.c.

* * *

Struggle to the fake news: from the state of the art to a regulatory perspective for "digital living" on the sidelines of the Digital Services Act

Abstract: The article aims to offer a starting point for reflection on the current regulatory framework of the struggle to the fake news phenomenon and the dangers it entails, with the dual purpose of identifying the aspects of strength and fragility that the current regulatory framework offers and to identify the best way to better protect the subjects involved. Credit is given to the EU legislator for having prepared the dual proposal for regulation of the DSA and DMA and for having had the courage to affirm its sovereignty in the field of digital relationships, with the hope that the approval process will lead also to the enhancement of a multi-stakeholder governance approach for self-regulation and to establish a specific guarantor authority to combat the phenomenon of *private censorship* too.

Keywords: Fake news – Info-war – Protection of rights – Information Guarantor Authority

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0082
Articolo sottoposto a peer review

Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'*Artificial Intelligence Act* dell'Unione europea

Daniele Chiappini

I sistemi di Intelligenza Artificiale sono ormai utilizzati in ambiti sempre più numerosi e recentemente sono stati impiegati anche nel campo medico e giuridico, ivi compreso quello penale. La diffusione di tali sistemi crea la necessità di regolamentarli, soprattutto in relazione agli aspetti di responsabilità civile. Partendo dalla descrizione della genesi del quadro giuridico dell'Unione europea in materia, in questo articolo si intende fornire una prospettiva sulla futura regolamentazione sulla responsabilità civile dei sistemi di Intelligenza Artificiale, tenendo in considerazione la questione della definizione di IA e le classificazioni effettuate tra IA ad alto rischio e altre Intelligenze Artificiali. Il quadro così risultante viene posto in relazione con la proposta di Regolamento contenuta nell'*Artificial Intelligence Act* della Commissione europea al fine di valutarne le correlazioni e le discrepanze e avere un quadro definito circa i possibili sviluppi della materia.

Responsabilità civile – Intelligenza Artificiale – Unione europea

Sommario: *1. Introduzione – 2. Genesi del quadro giuridico europeo – 3. La regolamentazione della responsabilità civile dell'IA in Europa – 3.1. Definizione di Intelligenza Artificiale – 3.2. Sistemi ad alto rischio – 3.3. Altri sistemi di IA – 3.4. Pratiche di IA vietate – 4. Conclusioni*

1. Introduzione

Il concetto di Intelligenza Artificiale (IA) è ormai di comune utilizzo ed è possibile trovare applicazioni che usano o si basano su questa tecnologia in molti ambiti. Non sorprende dunque rilevare che negli ultimi anni l'attenzione dei legislatori europei, come anche di quelli nazionali ed extraeuropei, si stia concentrando anche sulla regolamentazione delle applicazioni in oggetto. Sebbene infatti dal punto di vista storico l'interesse nei confronti dell'IA è stato altalenante, è nell'ultimo decennio che si è avuto uno sviluppo di questa tecnologia mai visto in precedenza, sviluppo che l'ha portata ad essere utilizzata e commercializzata in numerosi ambiti, fino a raggiungere contesti completamente nuovi, come ad esempio quello giudiziario[1].

L'incremento dell'utilizzo dell'Intelligenza Artificiale ha portato alcuni analisti a stimarne il potenziale valore di mercato in 150 miliardi di dollari[2] e tale espansione ha comportato, conseguentemente, l'emergere di aspetti problematici dal punto di vista giuridico, tra i quali quelli relativi alla definizione della responsabilità nel caso in cui vengano cagionati danni da sistemi di Intelligenza Artificiale.

Il problema centrale è rappresentato dal fatto che più l'IA è in grado di prendere decisioni autonome, meno questa può essere considerata come uno strumento nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore ecc.). Que-

D. Chiappini è avvocato, assegnista di ricerca presso il CNR e dottorando presso il Dipartimento di Medicina dell'Università degli Studi di Perugia, *curriculum* Diritto scienza ed etica.

sto, a sua volta, comporta la necessità di valutare se le regole ordinarie in materia di responsabilità siano adeguate o se sia invece necessario prevedere la creazione di nuovi principi e norme volte a chiarire il soggetto a cui sia attribuibile la responsabilità per azioni e omissioni dannose imputabili all'Intelligenza Artificiale, qualora le cause non possano essere ricondotte a un soggetto umano specifico[3].

La questione appare di particolare importanza poi in tutti quegli ambiti in cui l'utilizzo di questa nuova tecnologia è correlata a diritti fondamentali, come, ad esempio, nel campo della giurisprudenza e della medicina. A titolo meramente esemplificativo ricordiamo come in quest'ultimo settore l'IA venga utilizzata nella diagnosi delle malattie[4], nella creazione di farmaci[5], nella valutazione dell'interazione tra farmaci stessi[6], nonché in molti altri campi tra i quali spicca anche la lotta al Coronavirus[7].

Questa crescita esponenziale delle applicazioni dell'Intelligenza Artificiale rende necessario dare una risposta alle questioni giuridiche sollevate da tale rivoluzione tecnologica. Un primo tentativo di fornire risposte a livello europeo è rappresentato dal percorso che dovrebbe portare all'approvazione di un Regolamento relativo alla responsabilità civile dell'IA, partendo dalla proposta inclusa nella Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale.

2. Genesi del quadro giuridico europeo

Il percorso che dovrebbe portare all'approvazione di un corpus normativo relativo alla regolamentazione dell'IA ha avuto inizio nel 2016, quando, il 31 maggio, è stato prodotto un primo progetto di relazione[8] da parte della commissione JURI del Parlamento europeo a seguito dell'audizione in Commissione di numerosi esperti in campi afferenti l'IA. In tale occasione la composizione della Commissione è stata integrata con membri delle Commissioni Industria, ricerca e energia, della Commissione mercato interno e protezione dei consumatori e della Commissione occupazione e affari sociali. Conseguentemente alla relazione, il Parlamento europeo ha poi adottato la Risoluzione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, del 16 febbraio 2017. Partendo da quanto esposto nella relazione della Commissione JURI, la Risoluzione ha affrontato la questione della responsabilità civile sia nei considerando (da Z. ad AI.) sia nel testo, intitolando un paragrafo "Responsabilità" comprendente gli articoli da 49 a 59. In tale contesto il Parlamento europeo ha espresso la centralità della responsabilità civile per ciò che concerne i danni causati dai robot (attribuendo alla parola robot un concetto più ampio, comprensivo di quello di Intelligenza Artificiale), auspicando un'analisi a livello di Unione al fine di garantire il medesimo livello di efficienza, trasparenza e coerenza nell'attuazione della certezza giuridica nell'interesse tanto dei cittadini e dei consumatori, quanto delle imprese[9]. Già nella risoluzione in oggetto si richiedeva alla Commissione di presentare una proposta di atto legislativo sulle questioni giuridiche relative allo sviluppo e all'utilizzo della robotica e dell'Intelligenza Artificiale, in associazione a strumenti non legislativi quali linee guida e codici di condotta. Riguardo a questi ultimi la Risoluzione presentava, in un allegato *ad hoc*, una proposta di codice etico-deontologico per gli ingegneri robotici, un codice per i comitati etici di ricerca, nonché due licenze, una per i progettisti e una per gli utenti. Interessante e degna di nota è anche la posizione assunta in relazione alla possibilità di attribuire una personalità[10], definita elettronica o artificiale, alle IA in modo simile a quanto previsto per le persone giuridiche[11], ipotesi che è stata in seguito abbandonata.

Alla Risoluzione è quindi seguito un follow-up da parte della Commissione europea[12] in cui il nodo centrale è rappresentato dal se e dal come adattare le norme aventi ad oggetto la responsabilità civile alle esigenze dell'economia digitale. La Commissione conclude con l'intenzione di collaborare con il Parlamento europeo e con gli Stati membri al fine di dare una risposta comune dell'Unione a questa sfida. Nel documento la Commissione ritiene strettamente correlata agli aspetti in oggetto anche la Direttiva sulla responsabilità dei danni da prodotto[13], che dovrà essere oggetto, si legge nel documento, di una valutazione, il cui scopo sarà quello di determinare se e in quale misura la Direttiva sia in grado di soddisfare i suoi obiettivi di garantire la responsabilità del produttore per i danni causati da un prodotto difettoso anche nell'ambito del danno prodotto dalle nuove tecnologie (ad esempio software, cloud computing, *Internet of Things*, robot avanzati, sistemi automatizzati e autonomi). Al riguardo la Commissione ha successivamente portato avanti una consultazione mirata con lo studio di valutazione d'impatto sulla possibile revisione della Direttiva[14].

Parallelamente al processo istituzionale, si è sviluppato un importante dibattito sulla questione che ha riguardato tanto l'aspetto della regolamentazione della responsabilità civile quanto quello della possibile creazione di un nuovo tipo di personalità giuridica. In particolare, riguardo quest'ultima, è stato rilevato che l'applicazione di strumenti dogmatici tradizionali alle conseguenze dell'utilizzo di sistemi

di Intelligenza Artificiale comporterebbe il rischio di far ricadere il danno sui soggetti danneggiati o sulla collettività, rendendo l'uso dell'IA un rischio collettivo[15]. Conseguentemente la possibile risposta sarebbe da ricercare nella creazione della suddetta personalità *ad hoc* per i sistemi di Intelligenza Artificiale, la cui questione è lungi dall'essere pacifica. Dal punto di vista pratico-funzionale-giuridico, il diritto può infatti attribuire soggettività a entità diverse creando delle *fictiones iuris*, come avviene nel caso delle persone giuridiche, e anche come è avvenuto in passato per altre tipologie di personalità[16]. Al riguardo però da più parti se ne è evidenziata l'infondatezza[17] o il rischio intrinseco[18], in quanto azzardo morale non applicabile a causa della differenza tra i processi decisionali umani e quelli artificiali. Nonostante quanto esplicitato dai sostenitori di questa posizione, la creazione di una personalità artificiale limitata[19] appare preferibile al fine di permettere una regolamentazione omnicomprensiva che possa anche guardare oltre al mero dato attuale e coprire eventuali avanzamenti tecnologici futuri. Ciò nonostante, tanto la dottrina maggioritaria quanto i decisori politici hanno preferito orientarsi sulla creazione di un sistema di responsabilità civile diretta dell'IA, attualmente una delle questioni maggiormente dibattute. Sul tema, infatti, la dottrina si domanda se le figure di responsabilità esistenti siano idonee a colmare le lacune prodotte dalle attività e dalle conseguenze di queste da parte dell'IA e quali risultino maggiormente applicabili[20], fornendo risposte in linea con quanto esplicitato dai successivi documenti e atti comunitari.

L'attività delle istituzioni dell'Unione, sulla base di quanto esplicitato dalla Risoluzione del 2017, ha quindi condotto alla produzione di numerosi atti, quali la Comunicazione *L'Intelligenza Artificiale per l'Europa*[21], il Piano coordinato sull'Intelligenza Artificiale[22], la Risoluzione su una politica industriale europea globale in materia di robotica e Intelligenza Artificiale[23], la Comunicazione *Creare fiducia nell'Intelligenza Artificiale antropocentrica*[24], per sfociare nel libro bianco sull'Intelligenza Artificiale[25]. A fianco di tali documenti sono poi stati prodotti numerosi studi e linee guida che hanno orientato la stesura dei numerosi atti legislativi adottati e in via di adozione. Ricordiamo a titolo esemplificativo ma non esaustivo il documento *Intelligenza Artificiale, robotica e sistemi autonomi* del gruppo europeo di etica delle scienze e delle nuove tecnologie[26], gli *Orientamenti etici per un'Intelligenza Artificiale affidabile* del Gruppo indipendente di Esperti di Alto livello sull'Intelligenza Artificiale[27], lo studio *Intelligenza Artificiale e responsabilità civile* richiesto dal Comitato JURI del Parlamento europeo[28]. In particolare, con gli orientamenti del gruppo di esperti di alto livello si è inteso promuovere un concetto di Intelligenza Artificiale affidabile basata su tre componenti: la legalità, in base alla quale l'IA deve ottemperare alle leggi e regolamenti ad essa applicabili, l'eticità, assicurando l'adesione a principi e valori etici e la robustezza, che deve sussistere sia dal punto di vista tecnico che sociale dato che i sistemi di IA sono in grado di causare danni non intenzionali. Ciascuna di tali componenti è un elemento necessario ma non sufficiente per realizzare un'IA affidabile, in quanto tutte e tre dovrebbero operare armonicamente durante l'intero ciclo vitale del sistema.

Nel libro bianco la Commissione, basandosi sui documenti precedentemente citati, definisce le opzioni strategiche su come raggiungere il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a determinati usi di tale tecnologia riconoscendo che, come ogni nuova tecnologia, anche questa è foriera tanto di opportunità quanto di rischi. Conseguentemente, vengono fatti propri dal libro bianco i sette requisiti fondamentali individuati negli orientamenti del gruppo di esperti di alto livello, ovvero: intervento e sorveglianza umana, robustezza tecnica e sicurezza, riservatezza e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e accountability.

Viene anche trattata la responsabilità civile nel paragrafo intitolato *Rischi per la sicurezza e per il funzionamento efficace del regime di responsabilità*. Nella sezione viene ribadito che la mancanza di disposizioni chiare in materia di sicurezza, capaci di affrontare i rischi che ogni transizione tecnologica porta con sé, può creare, oltre a pericoli per le persone interessate, incertezza giuridica per le imprese che commercializzano nell'Unione prodotti che integrano sistemi di IA. Conseguentemente viene specificato come la difficoltà di risalire al soggetto responsabile delle decisioni adottate da sistemi di IA sia una questione centrale, anche a causa di alcune delle caratteristiche proprie dell'Intelligenza Artificiale stessa, come l'opacità (il c.d. effetto "scatola nera"[29]). Ciò nonostante, la Commissione afferma che il vasto corpus di norme vigenti dell'UE in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi, ivi incluse le norme settoriali nonché quelle integrative poste dalle legislazioni nazionali, sia potenzialmente applicabile anche ai sistemi di IA, posizione condivisa anche dal Parlamento europeo.

La Commissione, quindi, specifica che coloro che subiscono un danno provocato da sistemi di Intelligenza Artificiale debbano godere dello stesso livello di protezione di coloro che subiscono danni causa-

ti da altre tecnologie, ma senza che questo comporti un blocco della ricerca e dello sviluppo tecnologico[30]. Diviene quindi necessario valutare attentamente tutte le opzioni che consentano di raggiungere tale obiettivo, compresa la possibilità di modificare la Direttiva sulla responsabilità per danno da prodotti difettosi o di compiere ulteriori interventi mirati di armonizzazione delle norme nazionali in materia di responsabilità. Partendo da tali considerazioni quindi vengono poste le basi dell'approccio europeo, il quale, mirando a raggiungere un equilibrio tra protezione dei soggetti danneggiati e salvaguardia dei produttori, e in particolare delle PMI del settore, segue un approccio basato sul rischio al fine di garantire la proporzionalità dell'intervento normativo, definendo criteri chiari[31] per distinguere le diverse applicazioni di IA, in particolare stabilendo quali sistemi rientrino nella categoria "ad alto rischio".

A seguito della pubblicazione del libro bianco si è acuito lo scambio interdisciplinare che ha visto partecipare non solo giuristi ed eticisti appartenenti a diverse specializzazioni normalmente non interloquenti, ma anche studiosi di altre scienze, sia umane che dure. In tal modo, è stato rilevato che si punta al superamento delle barriere esistenti tra le discipline al fine di elaborare una "lex robotica" volta a regolare i rapporti uomo-macchina e macchina-macchina nel rispetto dei diritti umani[32].

Tale approccio è stato confermato anche nella *Relazione sulle implicazioni dell'Intelligenza Artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*[33] in cui viene ribadito che «sebbene in linea di principio le norme vigenti dell'Unione e nazionali in materia di responsabilità siano in grado di far fronte alle tecnologie emergenti, le dimensioni e l'effetto combinato delle sfide poste dall'Intelligenza Artificiale potrebbero rendere più difficile offrire alle vittime un risarcimento in tutti i casi in cui ciò sia giustificato. Pertanto, l'allocazione dei costi in caso di danni può risultare ingiusta o inefficiente in base alle norme vigenti. Per ovviare a questa situazione e affrontare le potenziali incertezze del quadro vigente, gli adeguamenti della Direttiva sulla responsabilità per danno da prodotti difettosi e dei regimi nazionali in materia di responsabilità dovrebbero utilizzare un approccio basato sul rischio, vale a dire tenendo conto del fatto che le diverse applicazioni dell'intelligenza artificiale presentano rischi diversi»[34].

Successivamente è stata anche lanciata una pubblica consultazione sul Libro bianco che ha permesso a Stati membri, istituzioni, industria, parti sociali, ricercatori e portatori di interessi di esprimere il proprio punto di vista. I risultati della consultazione[35] sono stati utilizzati per proporre una revisione del Piano coordinato sull'IA.

Contemporaneamente agli aspetti appena descritti, sono state portate avanti numerose attività volte alla regolamentazione di differenti fattispecie inerenti all'utilizzo dell'Intelligenza Artificiale da parte del Parlamento europeo. Tali attività hanno riguardato, ad esempio, questioni inerenti alla proprietà intellettuale, ad aspetti penali e a profili etici, nonché l'ambito della responsabilità civile, con l'adozione di una risoluzione in materia[36] a cui è seguita la redazione della *Relazione sull'Intelligenza Artificiale in un'era digitale*[37], fatta propria dal Parlamento europeo nel maggio 2022 con una nuova Risoluzione[38]. Merita di essere citato il fatto che, in quest'ultima, il Parlamento europeo ha invitato la Commissione[39], laddove intenda proporre nuove normative digitali in settori come l'IA, a utilizzare proposte che prevedano l'adozione di atti legislativi esclusivamente in forma di Regolamenti.

Attraverso la risoluzione sulla responsabilità civile, il Parlamento ha chiesto alla Commissione di presentare una proposta di regolamento sulla materia seguendo le raccomandazioni incluse nell'allegato alla risoluzione stessa.

Dal punto di vista della definizione di IA, in diversi atti si cerca di chiarire il concetto di Intelligenza Artificiale dal punto di vista giuridico. Questa statuizione, ovviamente necessaria, rappresenta un importante elemento, in quanto dal punto di vista giuridico, ma anche da quello tecnico-scientifico, la risposta al quesito "cosa sia l'intelligenza artificiale" non è univoca, non esistendone una definizione generalmente accettata. La risoluzione del Parlamento europeo sulle norme di diritto civile sulla robotica proponeva definizioni comuni per i sistemi *cyber* fisici, sistemi autonomi, robot autonomi intelligenti e relative sottocategorie prendendo in considerazione specifiche caratteristiche di un robot intelligente[40].

Nel documento *L'Intelligenza artificiale per l'Europa*[41] e nel *Piano coordinato sull'intelligenza artificiale*[42], la Commissione considera ricompresi nella definizione di Intelligenza Artificiale tutti i sistemi che mostrano comportamenti intelligenti analizzando il loro ambiente e agendo, con un certo grado di autonomia, per il raggiungimento di obiettivi specifici. Questi sistemi possono essere puramente basati su software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software di analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure l'intelligenza artificiale può essere integrata in dispositivi hardware (ad esempio robot avanzati, auto autonome, droni o applicazioni *Internet of Things*)[43]. Tali definizioni sono state successi-

vamente modificate (vedi *infra*). Per completezza riteniamo opportuno specificare che alcuni organismi, comitati e commissioni di altri Paesi hanno inteso definire differentemente l'Intelligenza Artificiale. Ad esempio, il rapporto *Artificial Intelligence and Robotics*[44] del Comitato per la scienza e la tecnologia della Camera dei Comuni del Parlamento del Regno Unito, riconosce che c'è una tendenza a descrivere l'IA mettendola in contrasto con l'intelligenza umana e sottolineando che la prima non appare in natura[45]. Il Comitato non fornisce una definizione specifica di IA, e ciò è coerente con l'approccio del documento, che preferisce non creare regole *ad hoc* ma affida la valutazione degli aspetti etici, legali e di governance a una specifica Agenzia. Allo stesso modo, il documento statunitense *Preparing for the future of Artificial Intelligence*[46], esteso dall'Ufficio esecutivo del Presidente degli Stati Uniti d'America, Comitato nazionale per la scienza e la tecnologia, dedica un intero paragrafo alla domanda "cos'è l'intelligenza artificiale", ma conclude solo che non esiste una definizione universalmente accettata e offre solo diverse classificazioni di IA relative a sistemi esistenti[47].

3. La regolamentazione della responsabilità civile dell'IA in Europa

La proposta di regolamento, contenuta nella risoluzione del Parlamento UE, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale del 2020, si pone come obiettivo la definizione di un quadro giuridico certo in materia di responsabilità civile. Tale quadro rientra nella politica comunitaria volta alla costruzione di un'Intelligenza Artificiale che sia sicura ed affidabile e punta a instaurare un clima di fiducia verso la stessa. Quello della fiducia, secondo quanto previsto dalla proposta, è infatti un elemento fondamentale in quanto «qualsiasi quadro giuridico in materia di responsabilità civile orientato al futuro deve infondere fiducia nella sicurezza, nell'affidabilità e nella coerenza di prodotti e servizi, compresa la tecnologia digitale, al fine di trovare un equilibrio tra l'efficace ed equa tutela delle potenziali vittime di danni o pregiudizi e, allo stesso tempo, la disponibilità di una sufficiente liberta d'azione per consentire alle imprese, in particolare alle piccole e medie imprese, di sviluppare nuove tecnologie e nuovi prodotti o servizi»[48]. In tal modo viene ribadito che l'obiettivo di qualsiasi regolamentazione in materia di responsabilità debba essere quello di garantire la certezza del diritto per tutte le parti coinvolte, emanando, in tutto il territorio dell'Unione europea, una legislazione uniforme fondata su un quadro giuridico orizzontale e armonizzato, da cui discende la forma scelta, ovvero quella del Regolamento, in grado di fornire regole comuni obbligatorie per tutti i soggetti dell'unione, dagli Stati ai cittadini.

La normativa relativa alla responsabilità civile per danni cagionati dall'Intelligenza artificiale non poserebbe però esclusivamente su questo strumento. Nella proposta vi è infatti un importante rinvio alla Direttiva sulla responsabilità per danno da prodotti difettosi che rappresenterebbe il secondo elemento del quadro europeo sulla responsabilità civile per l'IA. Ricordiamo che tale direttiva è integrata a livello nazionale da quadri non armonizzati in materia di responsabilità civile e che prevede una tutela ulteriore che la sola responsabilità per colpa prevista a livello nazionale non è in grado di fornire introducendo un regime di responsabilità oggettiva del produttore per i danni causati dai difetti del prodotto.

A tale riguardo, la proposta contiene anche la valutazione circa la necessità di un adeguamento o della trasformazione in regolamento[49] della Direttiva in oggetto, posizione condivisa anche dal Parlamento UE[50] nell'ultima Risoluzione approvata.

Il Parlamento europeo, nell'approvare la *Risoluzione sull'Intelligenza Artificiale in un'era digitale*, basandosi sulla relazione della Commissione speciale sull'Intelligenza Artificiale nell'era digitale (AIDA)[51], ha infatti sottolineato che la direttiva sulla responsabilità per danno da prodotti difettosi e i regimi nazionali di responsabilità per colpa possono, in linea di principio, rimanere il fulcro della legislazione per contrastare la maggior parte dei danni provocati dall'IA[52] riconoscendo però che, per poter fare ciò, sarà necessario operare alcune modifiche[53]. Tali cambiamenti saranno volti in particolare ad aggiornare le definizioni giuridiche di "prodotto", al fine di comprendere applicazioni software integrate, servizi digitali e dipendenza tra prodotti, e di "produttore", al fine di includere gli operatori di back end, i fornitori di servizi e i fornitori di dati e per assicurare il risarcimento dei danni causati da tali tecnologie. Viene anche sottolineato, tuttavia, che è necessario evitare un approccio eccessivamente ampio o eccessivamente ristretto quando si compiono tali modifiche.

Terzo pilastro della costruenda disciplina sulla responsabilità civile dell'IA può essere considerato la proposta di regolamento presentata dalla Commissione europea nel così detto *Artificial Intelligence Act*, del 21 aprile 2021[54] volto all'armonizzazione delle normative sull'Intelligenza Artificiale che sarà posto in votazione in prima lettura all'Europarlamento, a settembre 2022 attraverso la procedura legislativa

ordinaria. Nel memorandum viene infatti specificato come gli stessi elementi e tecniche che sono alla base dei benefici socioeconomici prodotti dall'IA possono anche comportare nuovi rischi o conseguenze negative per gli individui o la società, per cui, alla luce della velocità con cui si sviluppano le nuove tecnologie e delle conseguenti sfide che vengono poste in essere, l'Unione europea si impegna a perseguire un approccio equilibrato volto a preservare la leadership tecnologica dell'Unione e a garantire che gli europei possano beneficiare delle nuove tecnologie sviluppate e funzionanti secondo i valori, i diritti e i principi fondamentali dell'Unione stessa[55].

Tale proposta non regolamenta aspetti inerenti alla responsabilità civile dell'IA, ma si pone obiettivi specifici, come precedentemente proposto dalla risoluzione del Parlamento europeo sugli aspetti etici per l'IA, la robotica e le tecnologie correlate[56], ovvero:

- garantire che i sistemi di IA immessi sul mercato dell'Unione siano sicuri e rispettino la legislazione esistente sui diritti fondamentali nonché i valori dell'Unione;
- garantire la certezza del diritto per facilitare gli investimenti e l'innovazione nell'ambito dell'IA;
- migliorare la governance e l'effettiva applicazione della legislazione esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA che siano rispettose della legge, sicure e affidabili nonché prevenire la frammentazione del mercato.

Tale proposta di regolamento, pur non affrontando direttamente la questione della responsabilità civile dell'Intelligenza Artificiale, è importante e deve essere tenuta in considerazione in quanto tratta alcuni elementi presenti anche nella risoluzione del Parlamento europeo che propone l'adozione di un regolamento sulla responsabilità civile, e che quindi costituiscono un punto di partenza comune da valutare quando si imposta la discussione su tale ambito, come specificato dalla proposta stessa[57]. In particolare, le questioni di interesse affrontate riguardano la definizione di Intelligenza Artificiale, la categorizzazione dei sistemi di IA e la determinazione di quali siano le pratiche di Intelligenza Artificiale vietate. Per tale motivo si terrà in considerazione la proposta della Commissione per valutare, *mutatis mutandis*, come potrebbe essere implementata quella relativa al regime di responsabilità civile.

Quindi, al fine di fornire una visione di quella che potrebbe essere la regolamentazione della responsabilità civile dell'IA, vengono presi in considerazione tre strumenti. Il primo è l'*Artificial Intelligence Act*, una proposta di Regolamento della Commissione europea del 2021 che, nel momento in cui si scrive, è in discussione al Parlamento europeo secondo la procedura legislativa ordinaria. In tale atto la Commissione adotta un approccio basato sul rischio multilivello prevedendo una categorizzazione dei sistemi di IA e una serie di norme correlate, occupandosi di regolamentare la sicurezza di tali sistemi in una prospettiva *ex ante*. Il secondo strumento invece è la Risoluzione del Parlamento europeo concernente la responsabilità civile dell'IA del 2020 che contiene una proposta di regolamento sulla materia volta a regolamentare la responsabilità civile, ma la cui proposta dovrà essere formalizzata dalla Commissione e potrebbe essere quindi modificata, come già avvenuto con la risoluzione alla base dell'AI Act. Merita di essere sottolineato il fatto che, in conseguenza di tale modifica, i due strumenti attualmente non sono completamente coerenti dal punto di vista delle definizioni. Il terzo strumento è rappresentato dalla modificanda direttiva sui danni da prodotto.

Tornando alla proposta di regolamento contenuta nella Risoluzione del Parlamento europeo, la questione si innesta attorno alla necessità di individuare il rischio legato all'utilizzo dei sistemi di Intelligenza Artificiale, nonché alla corretta allocazione delle responsabilità fra i diversi soggetti che intervengono dalla scrittura dell'algoritmo fino all'utilizzo dello stesso da parte dell'utente.

È proprio su questi elementi che la proposta di regolamento del Parlamento trova un punto di collegamento con quanto presentato dalla Commissione nell'*Artificial Intelligence Act*, in relazione alla categorizzazione delle tipologie di IA. Nella risoluzione del Parlamento europeo si propone alla Commissione l'adozione di un regime di responsabilità oggettiva per i sistemi ad alto rischio mentre per gli altri sistemi è prevista l'applicazione di un regime di responsabilità per colpa nonché il rinvio ad alcune delle norme vigenti nei paesi membri.

La bozza di Regolamento è strutturata su un totale di cinque capi e quindici articoli a cui sono anteposti ventiquattro considerando. Nelle disposizioni generali (Capo I) si individua l'oggetto, l'ambito di applicazione e si forniscono le definizioni, in maniera coerente con quanto presentato nell'*Artificial Intelligence Act*. Nel Capo II si definisce la responsabilità sussistente per i sistemi di IA ad alto rischio mentre il regime di responsabilità applicabile agli altri sistemi è sancito nel Capo III.

3.1. Definizione di Intelligenza Artificiale

Come già accennato in precedenza, non vi è un'unica definizione di Intelligenza Artificiale sia dal punto di vista giuridico che scientifico. In particolare, abbiamo già visto le definizioni che negli anni passati sono state adottate tanto dal Parlamento europeo quanto dalla Commissione europea, nonché da altre istituzioni non europee. La proposta contenuta nella risoluzione del Parlamento europeo del 2020 modifica la definizione di IA che lo stesso aveva dato nel 2017.

In tale data, infatti, la risoluzione prendeva in considerazione[58] la sussistenza delle seguenti caratteristiche al fine di circoscrivere cosa potesse essere definito Intelligenza Artificiale:

- ottenimento di autonomia grazie a sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività) e lo scambio e l'analisi di tali dati;
- l'autoapprendimento dall'esperienza e attraverso l'interazione (criterio facoltativo);
- almeno un supporto fisico minore;
- l'adattamento del proprio comportamento e delle proprie azioni all'ambiente;
- l'assenza di vita in termini biologici.

La proposta di regolamento contenuta nella risoluzione del Parlamento europeo sulla responsabilità civile in materia di IA invece definisce un "sistema di intelligenza artificiale (IA)" come «sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici»[59].

È interessante notare che la stessa definizione è stata approvata dal Parlamento europeo nella risoluzione del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate[60], ma la Commissione europea, nell'esercitare l'iniziativa legislativa per l'*Artificial Intelligence Act*, ha proposto una definizione differente di Intelligenza Artificiale in cui per "sistema di intelligenza artificiale" si deve intendere «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I e che può, per una data serie di obiettivi definiti dall'uomo, generare risultati quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono»[61].

Appare dunque plausibile ritenere che nella futura proposta di Regolamento che sarà presentata dalla Commissione europea in materia di responsabilità dell'IA verrà adottata la stessa definizione o sarà effettuato direttamente un richiamo a quella contenuta nell'*Artificial Intelligence Act*. Trattandosi in ogni caso di un atto *de iure condendo*, deve essere considerato che Parlamento e Consiglio potrebbero ritenere opportuno modificare tale definizione, tornando a quella proposta dal Parlamento stesso o approvandone una diversa dalle due qui esposte.

La proposta della Commissione differisce da quella del Parlamento in quanto definisce sistema di intelligenza artificiale un software, mentre il Parlamento UE prende in considerazione anche l'integrazione con sistemi hardware. Dal punto di vista della determinazione del concetto di IA quest'ultimo si riferisce a un generico "mostrare comportamenti che simulano l'intelligenza" e indicando alcuni dei mezzi tramite i quali questo avviene, lasciando dunque ampia discrezionalità all'interprete, mentre la prima correla la sussistenza del sistema di IA al fatto che quest'ultimo sia sviluppato attraverso una delle tecniche incluse nell'allegato I. Dal punto di vista degli obiettivi la proposta del Parlamento europeo prende in considerazione il raggiungimento di obiettivi specifici, mentre quella della Commissione indica quali sono i risultati attesi, ovvero contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono.

Sulla base di tale *excursus* possiamo ritenere la proposta della Commissione più completa e suscettibile di adeguamenti più semplici, data la previsione contenuta nel titolo X che permette alla Commissione di adottare atti di esecuzione volti a garantire l'applicazione uniforme del regolamento o atti delegati per aggiornare o integrare gli elenchi di cui agli allegati da I a VII[62]. La mancata specificazione dell'integrazione con sistemi hardware, presente nella risoluzione del Parlamento europeo, può essere ritenuta non indispensabile in quanto l'utilizzo del sistema di IA sviluppato secondo quanto previsto dal discutendo regolamento da parte del sistema hardware, permette di applicare la normativa in oggetto anche ai sistemi integrati hardware-software.

3.2. Sistemi ad alto rischio

In linea con l'approccio scelto, basato sulla gestione del rischio, l'utilizzo e la creazione di sistemi di IA ad alto rischio è consentito sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e a una valutazione di conformità *ex ante*. La classificazione di un sistema di IA come ad alto rischio non dipende solo dalla funzione svolta dal sistema stesso, ma anche dallo scopo specifico e dalle modalità per le quali tale sistema viene utilizzato[63].

Per ciò che concerne la definizione di sistemi di IA ad alto rischio, terremo in considerazione quella con-

tenuta nella proposta di regolamento della Commissione (*Artificial Intelligence Act*) in quanto non solo più recente, ma anche frutto dell'elaborazione della Commissione partendo dalla risoluzione del Parlamento europeo sugli aspetti etici dell'IA, da un lato, e in quanto proposta ufficiale elaborata dall'unico organo cui compete l'iniziativa legislativa dall'altro. Tale proposta individua come sistemi ad alto rischio quei sistemi che operano in modo autonomo e presentano un potenziale significativo di causare danni o pregiudizi a una o più persone in modo casuale e che va oltre quanto ci si possa ragionevolmente aspettare. L'importanza del potenziale dipende dall'interazione tra la gravita dei possibili danni o pregiudizi, dal grado di autonomia decisionale, dalla probabilità che il rischio si concretizzi e dalla modalità e dal contesto di utilizzo del sistema di IA[64]. Per poter essere ricompreso nei sistemi ad alto rischio, l'IA deve essere inclusa nell'elenco presente nell'allegato al Regolamento, in relazione al quale viene conferito alla Commissione il potere di adottare atti delegati al fine di modificarlo secondo le necessità, inserendo nuovi tipi di sistemi di IA ad alto rischio e settori fondamentali in cui sono utilizzati, eliminando tipi di sistemi di IA che non possono più essere considerati ad alto rischio e modificando i settori fondamentali per i sistemi di IA ad alto rischio esistenti[65]. Per tali tipi di sistemi è previsto l'obbligo di stipulare idonea copertura assicurativa per la responsabilità civile, concretizzando una tutela che era già stata paventata nella risoluzione del 2017[66].

Circa i requisiti necessari affinché un'IA sia inserita nell'allegato, e risulti quindi ad alto rischio, la risoluzione del Parlamento europeo non contiene elementi utili a tale definizione, ma questo è ovviato dall'*Artificial Intelligence Act*, che specifica che un sistema di IA debba essere considerato ad alto rischio in due casi. Il primo è rappresentato dalla situazione in cui siano soddisfatte contemporaneamente due condizioni[67]. La prima è che il sistema sia destinato a essere utilizzato come componente di sicurezza di un prodotto, o sia esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II dell'atto. La seconda condizione prevede che il prodotto il cui componente di sicurezza sia un sistema di intelligenza artificiale, o lo stesso sistema di IA sia il prodotto, debba essere sottoposto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio.

Oltre a questo primo caso, sono poi considerati ad alto rischio anche i sistemi di IA inclusi nell'allegato III della risoluzione. Sulla base di tali elementi sono considerati sistemi ad alto rischio, inclusi nell'allegato III della proposta, applicazioni appartenenti a numerosi campi. A titolo esemplificativo ricordiamo *in primis* quelle di identificazione biometrica e categorizzazione delle persone fisiche e quelle applicate alla gestione e funzionamento delle infrastrutture critiche come la gestione del traffico o la fornitura dell'acqua. Quelle relative a istruzione e formazione professionale volte a determinare l'accesso a istituti di formazione o alla valutazione degli studenti nonché i sistemi utilizzati per determinare l'assunzione, la selezione e la promozione di persone fisiche in posti di lavoro. Quelle destinate a determinare l'accesso e la fruizione di servizi privati essenziali e di benefici pubblici, quali quelle che determinano l'affidabilità creditizia o la valutazione della possibilità di accedere a benefici pubblici assistenziali nonché i sistemi utilizzati per stabilire priorità di invio di servizi di primo intervento. Nell'ambito dell'applicazione della legge rientrano nella categoria ad alto rischio i sistemi destinati a compiere valutazioni relative al rischio di recidiva di una persona o di essere potenziale vittima di reati, quelli utilizzati con i poligrafi o per rilevare lo stato d'animo di una persona, quelli utilizzati per valutare l'affidabilità delle prove o per prevedere il verificarsi o il ripetersi di reati sulla base della profilazione di persone fisiche. Rientrano nella stessa categoria anche i sistemi utilizzati per la gestione della migrazione, dell'asilo e del controllo transfrontaliero, nonché, nell'ambito dell'amministrazione della giustizia, quelli volti ad assistere l'autorità giudiziaria nell'interpretazione dei fatti e nella ricerca della legge applicabile.

Tali sistemi ad alto rischio sono sottoposti a norme prescrittive che utilizzano un approccio simile a quello applicato nel Regolamento generale sulla protezione dei dati prevedendo che venga compiuta una valutazione del rischio, che i *dataset* utilizzati siano di alta qualità, che i risultati siano tracciabili, che siano rispettate le norme sulla documentazione tecnica, l'archiviazione dei dati e sulla trasparenza e che vi sia una supervisione umana e un alto livello di robustezza, sicurezza e accuratezza[68].

In questi casi la previsione attorno alla quale si impernia il regime di responsabilità extracontrattuale è quella secondo la quale il soggetto responsabile per danni o pregiudizi causati dall'attività di un sistema di intelligenza artificiale è l'operatore. Tale scelta è ricaduta su questo soggetto in quanto la responsabilità dell'operatore è apparsa giustificata dal fatto che è costui che controlla il rischio associato al sistema di IA, in modo analogo a quello che fa il proprietario di un'automobile. In tal modo il Parlamento europeo ritiene che, vista la complessità e il potenziale di connettività di un sistema di IA, l'ope-

ratore sarà, in molti casi, il primo punto di contatto per la persona interessata[69].

Per operatore si intende sia quello di front-end sia quello di back-end, a condizione che la responsabilità di quest'ultimo non sia già coperta dalla Direttiva sulla responsabilità per danni da prodotti difettosi (85/374/CEE)[70]. Per operatore di front-end si intende la persona fisica o giuridica che esercita un certo grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA e che beneficia del suo funzionamento[71], mentre per operatore di back-end si intende la persona fisica o giuridica che, su base continuativa, definisce le caratteristiche della tecnologia e fornisce i dati e il servizio di supporto di back-end essenziale e pertanto esercita anche un elevato grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA[72].

Nel Capo IV è stabilito che in presenza di più operatori, gli stessi saranno da considerarsi responsabili in solido[73]. Laddove ricorra tale ipotesi, al fine di individuare le rispettive quote di responsabilità, queste dovranno essere assegnate in considerazione del rispettivo grado di controllo che ciascun operatore ha esercitato sul rischio connesso all'operatività e al funzionamento del sistema di IA, dovendosi attuare il recupero delle rispettive quote attraverso il meccanismo dell'azione di regresso[74]. È inoltre previsto che, qualora il danno o il pregiudizio venga causato sia da un sistema di IA, attraverso un'attività, dispositivo o processo fisico o virtuale, sia da azioni di una persona interessata o di altro soggetto di cui la persona interessata sia responsabile, il grado di responsabilità dell'operatore debba essere ridotto di conseguenza. L'operatore non è poi ritenuto responsabile qualora la responsabilità del danno o del pregiudizio causato sia esclusivamente imputabile alla persona interessata o alla persona di cui questa è responsabile[75].

Dal punto di vista dell'elemento soggettivo, nel caso dei sistemi di IA ad alto rischio, viene sancito l'utilizzo di un criterio di responsabilità oggettiva[76], scelta avallata anche dal Parlamento europeo nella *Risoluzione sull'Intelligenza Artificiale in un'era digitale*[77]. Al riguardo è previsto che gli operatori di sistemi di IA ad alto rischio non possano eludere la responsabilità sostenendo di avere agito con la dovuta diligenza o che il danno o il pregiudizio sia stato cagionato da un'attività, dispositivo o processo autonomo guidato dal loro sistema di IA, ma non possono essere considerati responsabili qualora il danno o il pregiudizio sia dovuto a cause di forza maggiore[78]. È inoltre previsto che le norme del regolamento prevalgano sui regimi nazionali di responsabilità in caso di discrepanze nella classificazione dei sistemi di IA[79].

Per ciò che concerne il risarcimento, il regolamento pone delle norme sia relativamente all'importo che all'entità dello stesso. Dal primo punto di vista, viene stabilito che l'operatore di un sistema di IA ad alto rischio responsabile per danni o pregiudizi ai sensi del Regolamento stesso potrà essere condannato al pagamento di fino a un massimo di 2 milioni di euro in caso di morte o danni alla salute o all'integrità fisica cagionati a terzi o fino a un massimo di 1 milione di euro in caso di danni patrimoniali cagionati a terzi. È poi sancita una previsione specifica anche in relazione alla possibilità di far valere anche in cumulo una responsabilità di tipo contrattuale[80].

In relazione all'entità del risarcimento vengono disposte norme precise al fine dell'individuazione della stessa, che prendono in considerazione i costi sostenuti e il pregiudizio pecuniario subito[81].

Circa il termine di prescrizione dell'azione risarcitoria, questo varia a seconda che il danno sia patrimoniale o non patrimoniale. Per questo ultimo, infatti, il termine di prescrizione dell'azione è fissato in trenta anni che decorrono dalla data in cui si è verificato il danno. Per ciò che concerne i danni patrimoniali, invece, è previsto, in alternativa al termine di cui si è appena detto, un termine prescrizionale speciale di dieci anni che decorrono dalla data in cui si è verificato il danno al patrimonio. Tra i due così enunciati troverà applicazione il termine che scadrà per primo[82]. Rimangono applicabili le norme del diritto nazionale disciplinanti gli istituti della sospensione e dell'interruzione della prescrizione.

3.3. Altri sistemi di IA

Per quello che riguarda gli altri sistemi di IA, ovvero quelli che non vengono qualificati come sistemi ad alto rischio, è previsto un regime di responsabilità per colpa per danni e pregiudizi causati da una attività, da un dispositivo o da un processo fisico o virtuale guidato attraverso uno strumento di Intelligenza Artificiale[83]. Anche in questo caso il Parlamento europeo ha ritenuto corretta[84] la scelta di impostare il regime di responsabilità per danni causati da intelligenze artificiali non ad alto rischio su una responsabilità per colpa.

È rilevante specificare che la proposta di Regolamento del Parlamento europeo prevede solo una differenziazione tra sistemi ad alto rischio ed altri sistemi di IA, mentre la proposta contenuta nell'*Artificial Intelligence Act* suddivide i sistemi in oggetto in quattro categorie[85], quelli a rischio inaccettabile, quelli ad alto rischio, quelli a rischio limitato e quelli a rischio minimo. Trattando di altri sistemi di IA, il Capo III della proposta del Parlamento europeo sem-

bra quindi ricomprendere gli ultimi due. Giova quindi esplicitare che per sistemi a rischio limitato[86] si intendono quei sistemi che presentano un chiaro rischio di manipolazione (ad esempio tramite l'uso di *chatbot*) in relazione al quale gli utenti devono essere consapevoli che stanno interagendo con una macchina. A tali sistemi, nell'*Artificial Intelligence Act* vengono quindi imposti requisiti di trasparenza specifici.

Per sistemi a rischio minimo[87] si intendono invece tutti gli altri sistemi di IA che possono essere sviluppati e utilizzati in base alla legislazione esistente senza ulteriori obblighi legali.

Anche in tale fattispecie il soggetto su cui incombe l'obbligo di risarcimento è l'operatore, per il quale rilevano le stesse definizioni e le relative regole illustrate per i sistemi di IA ad alto rischio (vedi *supra*). È però previsto che l'operatore non possa essere ritenuto responsabile qualora sia in grado di dimostrare che il danno o il pregiudizio siano stati arrecati per causa a lui non imputabile nei casi previsti dal regolamento, ovvero che il sistema di IA si sia attivato senza che l'operatore ne fosse a conoscenza e contemporaneamente siano state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione o nel caso in cui sia stata rispettata la dovuta diligenza nello svolgimento delle operazioni specificate nel Regolamento[88].

Per ciò che concerne il termine di prescrizione dell'azione risarcitoria e l'entità dei risarcimenti si rinvia espressamente alle leggi dello Stato membro in cui si è verificato il danno o il pregiudizio[89].

Appare quindi chiara la volontà del legislatore comunitario di assoggettare i sistemi di Intelligenza Artificiale che non appartengono alla categoria dei sistemi ad alto rischio ad un regime di responsabilità in cui, pur in un'ottica di armonizzazione comunitaria, trovino applicazione le regole già esistenti. Questo in quanto il Parlamento europeo ha ritenuto che il vigente diritto degli Stati membri in materia di responsabilità civile per colpa offra, il più delle volte, un livello sufficiente di tutela alle persone che subiscono danni a seguito dell'interferenza di un terzo, quale un hacker, o danni patrimoniali da parte di tale terzo, in quanto l'interferenza costituisce sistematicamente un'azione basata sulla colpa e solo in casi specifici, inclusi quelli in cui il terzo sia irrintracciabile o insolvibile, appaiono necessarie ulteriori norme in materia di responsabilità per integrare il diritto nazionale in materia di responsabilità civile[90].

3.4. Pratiche di IA vietate

La proposta di regolamento contenuta nella risoluzione del Parlamento europeo non prevede il riconoscimento di pratiche di IA vietate previste nel titolo II dell'*Artificial Intelligence Act* proposto dalla Commissione. Nonostante ciò, appare opportuno effettuare una rapida ricognizione di queste in quanto in grado di incidere anche nell'ambito di cui stiamo discutendo. La proposta di regolamento della Commissione prevede infatti una serie di pratiche di Intelligenza Artificiale vietate[91] in quanto contrarie ai principi dell'Unione e ai diritti fondamentali riconosciuti dalla stessa.

In primis è vietata l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che utilizzino tecniche subliminali al di là della consapevolezza di una persona al fine di falsarne in misura rilevante il comportamento e in modo tale da provocare, anche potenzialmente, un danno fisico o psicologico. È poi vietata l'immissione sul mercato, la messa in servizio o l'utilizzo di sistemi di IA capaci di sfruttare le vulnerabilità di un gruppo specifico di persone, a causa della loro età, disabilità fisica o mentale, con il fine di falsarne in misura rilevante il comportamento e provocare danni fisici o psicologici ai soggetti stessi o ad altri. È vietata l'immissione sul mercato, la messa in servizio o l'utilizzo di sistemi di IA da parte di autorità pubbliche o per loro conto, che siano in grado di valutare o classificare l'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o caratteristiche o della personalità, note o previste, mediante un punteggio sociale che determini uno o entrambi i seguenti elementi:

- un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non hanno alcun rapporto con i contesti con cui i dati sono stati originariamente generati o raccolti;
- un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche che sia sproporzionato rispetto alla gravità del loro comportamento sociale.

È altresì vietato l'utilizzo di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini dell'applicazione della legge. Tale divieto viene meno qualora tale uso risulti strettamente necessario per la ricerca mirata di potenziali vittime di crimini, inclusi i bambini scomparsi. Uno Stato membro può inoltre decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico per prevenire una specifica sostanziale e imminente minaccia alla vita o un attacco terroristico, nonché per permettere l'individuazione, la localizzazione, l'identificazione o il perseguimento di un autore o so-

spettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro del Consiglio 2002/584/GAI e punibile nello Stato membro interessato con una pena detentiva con massimo edittale di almeno tre anni, come stabilito dalla legislazione di tale Stato.

Per poter utilizzare i sistemi di identificazione biometrica in tali casi, vengono comunque definiti una serie di specifici requisiti[92], tra i quali spicca la necessità di un'autorizzazione preventiva emessa da un'autorità giudiziaria dello Stato membro in cui deve avvenire l'utilizzo. Riguardo questa fattispecie, merita di essere tenuto in considerazione il fatto che il Parlamento europeo, sottolineando che poiché molte tecnologie di identificazione basate su algoritmi attualmente in uso commettono errori di identificazione e di classificazione, danneggiando le persone che appartengono a determinati gruppi razziali o etnici, le persone LGBTI, i bambini, gli anziani e le donne e ricordando che gli individui non hanno soltanto il diritto a essere identificati correttamente ma anche di non essere identificati[93], ha chiesto un divieto permanente dell'utilizzo dei sistemi di analisi e/o riconoscimento automatici negli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali[94] e una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati, finche le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali e i risultati ottenuti siano privi di distorsioni e non discriminatori[95]. È quindi facilmente prevedibile che tale elemento sarà al centro della discussione per l'approvazione dell'atto.

Per ciò che concerne le violazioni[96] di queste disposizioni, la proposta di regolamento della Commissione europea prevede che gli Stati membri stabiliscano le norme relative alle sanzioni applicabili e adottino tutte le misure necessarie per assicurarne un'attuazione efficace, tenendo in particolare considerazione gli interessi dei piccoli fornitori e delle start-up nonché della loro redditività. È quindi previsto che gli Stati membri notifichino alla Commissione le norme adottate, nonché ogni modifica alle stesse.

È previsto, in caso di mancato rispetto del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5, nonché il caso di non conformità del sistema di IA ai requisiti di cui all'articolo 10 (dati e governance dei dati) che siano comminate sanzioni amministrative fino a 30.000.000 di euro o, qualora l'autore del reato sia una società, fino al 6% del suo fatturato annuo totale a livello mondiale, secondo quanto dichiarato nell'esercizio finanziario precedente.

La non conformità dei sistemi di IA a requisiti o obblighi diversi da quelli di cui agli articoli precedentemente menzionati è invece soggetta a sanzioni amministrative fino a 20.000.000 di euro o, se l'autore del reato è una società, fino al 4% del suo fatturato annuo totale a livello mondiale, secondo quanto emerge dall'esercizio finanziario precedente.

Laddove vengano fornite informazioni inesatte, incomplete o fuorvianti alle autorità competenti come risposta a una richiesta da parte delle stesse, il soggetto inadempiente è passibile di sanzioni amministrative fino a 10.000.000 di euro o, se l'autore del reato è una società, fino al 2% del suo fatturato annuo totale a livello mondiale, secondo quanto dichiarato nell'esercizio finanziario precedente.

Nel caso in cui sia possibile applicare entrambe le sanzioni precedentemente descritte nei tre casi menzionati, troverà applicazione quella di entità maggiore.

Al fine di determinare l'importo della sanzione per ciascun caso, devono essere valutate tutte le circostanze pertinenti della situazione specifica e in particolare la natura, la gravità e la durata della violazione e delle sue conseguenze. L'eventuale applicazione di sanzioni amministrative pecuniarie allo stesso operatore per la stessa infrazione da parte di altre autorità di vigilanza, nonché le dimensioni e la quota di mercato dell'operatore che ha commesso l'infrazione.

Al riguardo è interessante rilevare come le sanzioni in oggetto siano simili a quelle previste per la violazione del Regolamento Generale sulla Protezione dei Dati Personali (GDPR), che prevede sanzioni fino ad un massimo pari al 4% del fatturato annuo[97]. Possiamo quindi ritenere che, come le violazioni della privacy possono comportare anche un danno per l'interessato i cui dati sono stati violati, allo stesso modo la violazione delle regole che proibiscono l'utilizzo di sistemi di IA illustrate in questo paragrafo possono essere in grado di cagionare un danno a un soggetto. In questo caso, come anche nel caso della violazione del GDPR, riteniamo quindi che l'interessato potrà conseguentemente richiedere un risarcimento, secondo le regole previste dal discutendo regolamento sulla responsabilità civile dei sistemi di IA.

Concordemente con quanto espresso da autorevole dottrina[98], quello che si è illustrato è un modello che, per quanto tripartito, sembra riproporre, da un lato, quanto previsto dalla disciplina in tema di danno da prodotto difettoso, includendo nella fattispecie una nozione di prodotto e produttore in grado di ricomprendere i sistemi di IA e coloro che li sviluppano, applicando anche a questi il principio generale secondo cui i prodotti che non soddisfano le norme di sicurezza obbligatorie sono considerati difettosi

indipendentemente dalla colpa del produttore. Allo stesso modo questo tipo di responsabilità oggettiva viene riconosciuta sussistente anche in capo ad altri soggetti, in correlazione al tipo di sistema di IA utilizzato mentre risulta residuale, applicabile agli "altri sistemi di IA" un tipo di responsabilità per colpa.

4. Conclusioni

In conclusione, l'excursus appena compiuto non mostra altro che una parte del percorso in divenire che l'Unione europea sta compiendo nell'ambito della regolamentazione dell'Intelligenza Artificiale. Le proposte di regolamento del Parlamento europeo sulla Responsabilità civile dei sistemi di IA e quella della Commissione sull'*Artificial Intelligence Act*, sono solo alcuni punti di partenza, a cui si aggiungono, ad esempio, le risoluzioni e il lavoro compiuto circa la proprietà intellettuale e la responsabilità penale in ambito di sistemi di Intelligenza Artificiale.

Appare però chiaro come la pervasività di una regolamentazione della responsabilità civile dei sistemi di IA sia tale da incidere su numerosi campi ed ambiti del vivere comune. Se infatti la determinazione del framework etico, delle norme relative alla proprietà intellettuale e di quelle proprie dell'ambito penale trova una sua applicazione in campi e fattispecie specifiche, una regolamentazione della responsabilità civile appare essere ancora più necessaria in quanto in grado di tutelare i soggetti che vengono in contatto con tali sistemi, sempre più diffusi, attraverso la previsione di una cornice normativa aggiornata in grado di garantire il ristoro del danno subito. Allo stesso modo, tale previsione permetterà agli sviluppatori e alle aziende ICT di decidere come muoversi in questo campo. Si potrebbe ritenere che una regolamentazione stringente della responsabilità, ma anche degli aspetti etici, dei sistemi di IA possa comprimere l'attività inventiva e le possibilità che hanno le aziende di innovare, soprattutto rispetto a sistemi che non intendono applicare tali restrizioni. In realtà il progresso tecnologico non può avanzare a discapito della tutela dei diritti, ragion per cui non si può che salutare positivamente l'impegno dei legislatori, non solo comunitari, nel lavorare per stabilire norme in tale ambito.

Note

[1]Il governo estone ha istituito un programma pilota del Ministero della giustizia per automatizzare le sentenze dei tribunali per controversie di modesta (fino ad un massimo di 7.000,00).

[2]S. Chishti, I. Bartoletti, A. Leslie, S.M. Millie, *The AI Book: The artificial intelligence handbook for investors, entrepreneurs and FinTech visionaries*, Wiley & Sons inc., 2020, p. 79.

[3]Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, P8_TA(2017)0051, *Responsabilità*, lett. AB.

[4]Secondo un recente studio (X. Liu et al., *A comparison of deep learning performance against health-care professionals in detecting diseases from medical imaging: a systematic review and meta-analysis*, in "Lancet Digital Health", 2019, n. 1, p. 271.), l'Intelligenza Artificiale potrebbe essere in grado di diagnosticare le malattie con la stessa efficacia dei medici. Lo studio ha confrontato le prestazioni dell'IA e degli operatori sanitari nel rilevare le malattie utilizzando studi condotti tra il 2012 e il 2019. Secondo lo studio, le prestazioni diagnostiche sono risultate equivalenti e l'utilizzo di tecnologie di deep learning potrebbe rendere ancora più efficiente l'identificazione e malattie da parte dell'IA nei prossimi anni.

[5]Un farmaco usato per trattare il disturbo ossessivo compulsivo, la molecola DSP-1181, è stato creato da un'IA grazie agli sforzi congiunti di Exscientia e Sumitomo Dainippon Pharma. Tale farmaco è entrato nella sperimentazione clinica di Fase I in Giappone e il suo sviluppo ha richiesto un solo anno, contro i cinque anni di cui generalmente necessitano simili progetti. Inoltre, dai dati emerge anche che l'uso dell'IA per produrre farmaci possa comportare una diminuzione dei costi di ricerca e produzione.

[6]Sono stati creati degli algoritmi in grado di identificare le interazioni farmaco-farmaco a partire da contenuti generati dagli utenti come cartelle cliniche elettroniche e/o segnalazioni di eventi avversi. Altre fonti utilizzate sono i database come l'*FDA Adverse Event Reporting System* - FAERS e VigiBase dell'Organizzazione mondiale della sanità che consentono ai medici di inviare segnalazioni di possibili reazioni negative ai farmaci. A partire da questi dati, algoritmi di *deep learning* sono stati addestrati per analizzare tali report e individuare modelli che implicano interazioni tra farmaci.

[7]L'Intelligenza Artificiale è stata utilizzata in numerosi campi per combattere il coronavirus. In particolare, è stata utilizzata per predire, indentificare e tracciare la diffusione della malattia, per diagnosticare l'insorgenza della stessa nei pazienti tramite metodi non invasivi, per lo sviluppo di cure e vaccini (il vaccino Moderna è stato prodotto utilizzando anche algoritmi di IA) e in molti altri ambiti.

[8]Commissione JURI del Parlamento europeo, *Progetto di relazione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, 2016.

[9]Risoluzione del Parlamento europeo P8_TA(2017)0051, cit., art. 49.

[10]*Ivi*, art. 59, lett. F.

[11]D. Chiappini, *Artificial Intelligence and legal capacity, an introduction to robotic subjectivity*, in "Diritto e Processo", 2019, pp. 173-194.

[12]Risposta della Commissione europea alla Risoluzione Norme di diritto civile sulla robotica del 16 febbraio 2017, 2017.

[13]Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi.

[14]Lo studio è stato condotto per la direzione generale del mercato interno, dell'industria, dell'imprenditoria e delle PMI (DG GROW) della Commissione europea dal *Center for Strategy & Evaluation Services* - CSES e dai suoi partner Wavestone e CSIL. Gli esiti della consultazione sono disponibili sul sito della Commissione europea.

[15]G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, ESI, 2019, p. 27 ss.

[16]G. Taddei Elmi, *Soggettività artificiali e diritto*, in "Altalex", 25 giugno 2004.

[17]G. Taddei Elmi, A. Contaldo (a cura di), *Intelligenza Artificiale, Algoritmi giuridici Ius condendum o "fantadiritto"?*, Pacini giuridica, 2020, p. 83.

[18]*Ivi*, p. 178.

[19]G. Teubner, *Soggetti giuridici digitali?*, cit., p. 33 ss.

[20]G. Taddei Elmi, *Il* Quid*, il* Quomodo *e il* Quid iuris *dell'IA. Una riflessione a partire dal volume "Diritto e tecnologie informatiche"*, in questa Rivista, 2021, n. 2.

[21]Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, del 25 aprile 2018.

[22]Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Piano coordinato sull'Intelligenza Artificiale*, COM(2018) 795 final, del 7 dicembre 2018.

[23]Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale P8_TA(2019)0081.

[24]Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Creare fiducia nell'Intelligenza Artificiale antropocentrica*, COM(2019) 168 final, dell'8 aprile 2019.

[25]Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, 2020.

[26]European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and "Autonomous" Systems*, 2018.

[27]Gruppo indipendente di esperti ad alto livello sull'Intelligenza Artificiale, *Orientamenti etici per un'IA affidabile*, 2019.

[28]A. Bertolini, *Artificial Intelligence and Civil Liability*, Study requested by the JURI Committee of the European Parliament, 2020.

[29]Questo effetto è proprio di quegli algoritmi basati su tecniche di apprendimento automatico che osservando le caratteristiche degli utenti pronosticano una classe, un giudizio o suggeriscono decisioni senza che sia possibile spiegare come sono arrivate a quella determinazione.

[30]Commissione europea, *Libro bianco sull'intelligenza artificiale*, cit., p. 10.

[31]G. Taddei Elmi, S. Marchiafava, A. Unfer, *Responsabilità civile e personalità giuridica della Intelligenza Artificiale*, in "i-Lex", dicembre 2021, n. 2.

[32]A.F. Uricchio, G. Riccio, U. Ruffolo (a cura di), *Intelligenza Artificiale tra etica e diritti: prime riflessioni a seguito del libro bianco dell'Unione europea*, Cacucci, 2020.

[33]Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato Economico e Sociale europeo, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, COM(2020) 64 final, del 19 febbraio 2020.

[34]*Ivi*, *Conclusioni*, p. 19.

[35]Commissione Europea, *Consultazione sulla responsabilità civile – adeguare le norme in materia di responsabilità all'era digitale e all'intelligenza artificiale*, 18 ottobre 2021 - 10 gennaio 2022.

[36]Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, P9_TA(2020)0276.

[37]Commissione speciale sull'Intelligenza Artificiale in un'era digitale, *Relazione sull'Intelligenza Artificiale in un'era digitale*, cit.

[38]Risoluzione del Parlamento europeo del 3 maggio 2022 sull'Intelligenza Artificiale in un'era digitale, P9_TA(2022)0140.

[39]*Ivi*, cap. 4, lett. a), sez. i), art. 121.

[40]Risoluzione del Parlamento europeo P8_TA(2017)0051, art. 1.

[41]Comunicazione della Commissione COM(2018) 237 final, cit.

[42]Comunicazione della Commissione COM(2018) 795 final, cit.

[43]Comunicazione della Commissione COM(2018) 237 final, cit., cap. 1, *Introduzione – Accettare il cambiamento*, p. 1.

[44]House of Commons Science and Technology Committee, *Robotics and Artificial Intelligence*, 2016.

[45]*Ivi*, p. 5.

[46]Executive Office of the President National Science and Technology Council Committee on Technology, *Preparing for the future of Artificial Intelligence*, 2016.

[47]D. Chiappini, *Profili comparatistici nella regolamentazione dell'intelligenza artificiale: responsabilità, etica ed occupazione*, in "Nuovo Diritto Civile", 2018, n. 2.

[48]Risoluzione del Parlamento europeo P9_TA(2020)0276, cit., lett. B.

[49]*Ivi*, numero 8.

[50]Risoluzione del Parlamento europeo P9_TA(2022)0140, cit., cap. 4, lett. a), sez. iii), art. 143.

[51]Commissione speciale sull'Intelligenza Artificiale in un'era digitale, *Relazione sull'Intelligenza Artificiale in un'era digitale*, cit.

[52]Risoluzione del Parlamento europeo del 3 maggio 2022, P9_TA(2022)0140, cit., cap. 4, lett. a), sez. iii), art. 143.

[53]*Ivi*, art. 145.

[54]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 final, del 21 aprile 2021.

[55]*Ivi*, par. 1.2.

[56]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, P9_TA(2020)0275.

[57]Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., par. 1.2.

[58]Risoluzione del Parlamento europeo P8_TA(2017)0051, cit., art. 1.

[59]Risoluzione del Parlamento europeo P9_TA(2020)0276, cit., Allegato alla risoluzione: *Raccomandazioni dettagliate per l'elaborazione di un regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*, art. 3, co. 1, lett. a).

[60]Risoluzione del Parlamento europeo P9_TA(2020)0275, cit., art. 4, co. 1, lett. a).

[61]Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., art. 3, co. 1, n. 1.

[62]*Ivi*, art. 73.

[63]Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., p. 1.

[64]Risoluzione del Parlamento europeo P9_TA(2020)0276, Allegato alla risoluzione, cit., art. 3, lett. c).

[65]*Ivi*, art. 4, par. 2.

[66]Risoluzione del Parlamento europeo P8_TA(2017)0051, cit., artt. 58 ss.

[67]Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., art. 6.

[68]*Ivi*, Titolo II.

[69]Risoluzione del Parlamento europeo P9_TA(2020)0276, cit., n. 10.

[70] *Ivi*, Allegato alla risoluzione, cit., art. 3, lett. d).
[71] *Ivi*, art. 3, lett. e).
[72] *Ivi*, art. 3, lett. f).
[73] *Ivi*, art. 11.
[74] *Ivi*, art. 12.
[75] *Ivi*, art. 10.
[76] *Ivi*, art. 4, par. 1.
[77] Risoluzione del Parlamento europeo del 3 maggio 2022, P9_TA(2022)0140, cit., cap. 4, lett. a), sez. iii), art. 146.
[78] Risoluzione del Parlamento europeo P9_TA(2020)0276, Allegato alla risoluzione, cit., art. 4, par. 3.
[79] *Ivi*, art. 4, par. 5.
[80] *Ivi*, art. 5.
[81] *Ivi*, art. 6.
[82] *Ivi*, art. 7.
[83] *Ivi*, art. 8, par. 1.
[84] Risoluzione del Parlamento europeo del 3 maggio 2022, P9_TA(2022)0140, cit., cap. 4, lett. a), sez. iii), art. 146.
[85] Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, del 21 aprile 2021, par. 5.2.
[86] European Commission, New rules for Artificial Intelligence – Questions and Answers, April 2021.
[87] *Ibidem*.
[88] Risoluzione del Parlamento europeo P9_TA(2020)0276, Allegato alla risoluzione, cit., art. 8, par. 2.
[89] *Ivi*, art. 9.
[90] Risoluzione del Parlamento europeo P9_TA(2020)0276, cit., numero 9.
[91] Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., art. 5.
[92] *Ivi*, art. 5, par. 2.
[93] Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, P9_TA(2021)0405, art. 9.
[94] *Ivi*, art. 26.
[95] *Ivi*, art. 27.
[96] Proposta di Regolamento del Parlamento europeo e del Consiglio COM(2021) 206 final, cit., art. 71.
[97] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, *Regolamento Generale sulla protezione dei dati*, art. 83.
[98] G. Di Rosa, *Quali regole per i sistemi automatizzati intelligenti*, in "Rivista di diritto civile", 2021, n. 5, pp. 823-853.

* * *

Artificial intelligence and civil liability: regulatory perspective in the light of the EU Artificial Intelligence Act

Abstract: Artificial Intelligence systems are used in several applications. Recently they have been applied in the medical and legal fields, including the criminal one. Coherently with the diffusion of these systems, the need for their regulation has emerged, especially in the civil liability field. In this essay, we will provide a perspective of the future European regulation concerning the civil liability of artificial intelligence systems, starting from the genesis of the European Union legal framework on the subject. We will consider the issues of the AI definition and the classifications made between high-risk AI and other Artificial Intelligence types. The resulting framework is then compared to the Regulation proposal contained in the European Commission's Artificial Intelligence Act, to assess correlations and differences, and define possible developments of the matter.

Keywords: Civil liability – Artificial Intelligence – European Union

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0087
Articolo sottoposto a peer review

Profili di contrasto al cybercrime *in iure condito* e *de iure condendo*

Vittoria Sveva Zilia Bonamini Pepoli

Nell'era del digitale la nostra vita è ormai legata a doppio filo a smartphone e tablet che ci accompagnano in ogni nostro movimento. è proprio la natura itinerante di tali mezzi che li rende perfetti "contenitori" per accogliere i c.d. captatori informatici, ovvero i malware utilizzati a fini investigativi, per il perseguimento dei reati. In questo lavoro si approfondisce come la giurisprudenza e il legislatore abbiano cercato di regolare l'avvento di questi nuovi mezzi di ricerca della prova nel tentativo di trovare un bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati, previsto e tutelato dall'art. 112 Cost. relativo al principio dell'obbligatorietà dell'azione penale e l'art. 15 Cost., che sancisce il principio di inviolabilità della riservatezza e segretezza di qualsiasi forma di comunicazione. Al contempo, però, si vuole sottolineare come sia essenziale il contrasto al crimine informatico, attuato anche mediante l'utilizzo di tali strumenti e un adeguato sviluppo di risorse tecnologiche per la sicurezza informatica in grado di creare sistemi che siano "cyber resilienti". In tal senso, si porta alla luce la duplice natura, benevola e malevola, dello stesso mezzo: il malware.

Malware – Cybersecurity – Cybercrime – Diritto alla riservatezza – Captatore informatico

Sommario: *1. Introduzione – 2. I malware: l'anatomia, l'inserimento e i malware per i dispositivi mobili – 3. Gli aspetti giuridici internazionali ed europei sui reati informatici – 4. Il cybercrime:* in iure condito *e* de iure condendo *– 5. Conclusioni*

1. Introduzione

Il concetto di "bene informatico"[1] è stato usato per la prima volta in Italia negli anni '80 del Novecento in relazione ai dati, alle informazioni e ai programmi contenuti all'interno di un apparato informatico.

A lungo la dottrina e la giurisprudenza si sono interrogate se i beni in questione fossero assimilabili, ai fini della tutela penale, ai beni di natura corporale. Il quesito nasceva, in particolare, per quel che riguardava alcuni tipi di reati quali, ad esempio, il furto o il danneggiamento.

Ebbene, la risposta a tale quesito fu negativa per via dell'impossibilità di considerare come "beni corporali" quei beni che, in realtà, non sono tangibili. Infatti, la proprietà si riferisce a beni che abbiano natura corporale essendo impossibile fare riferimento agli stessi per i beni c.d. informatici[2].

La necessità di tutelare, proteggere ma, soprattutto, regolare il bene informatico nasce da un sempre maggiore sviluppo delle reti informatiche e della conseguente diffusione dei dispositivi elettronici portatili.

Lo sviluppo ha comportato una maggiore vulnerabilità dei sistemi e delle reti così da condurre a una doppia necessità: se da un lato è fondamentale avere una serie di norme a tutela e maggiore regolazione del bene giuridico di cui sopra, dall'altro si rende indispensabile la predisposizione di misure di sicurezza finalizzate a un controllo che stimoli l'utilizzo dei sistemi informatici e una sempre maggiore «libera circolazione delle informazioni»[3].

V.S. Zilia Bonamini Pepoli è dottoranda presso la Luiss Guido Carli, nel dottorato "Diritto e Impresa". Nel corso dell'a.a. 2015/2016 ha frequentato il Master di I livello in Cybercrime e informatica forense presso La Sapienza di Roma, Facoltà di Ingegneria dell'informazione, informatica e statistica.

L'utilizzo dei sistemi informatici e, in particolar modo, dei c.d. captatori informatici quale strumento investigativo, impone un contemperamento maggiore tra la tutela del diritto alla riservatezza e le esigenze di ordine pubblico.

Dopo la sentenza Scurato[4], il Legislatore ha parzialmente regolato l'uso del captatore informatico mediante l'introduzione del d.lgs. 29 dicembre 2017, n. 216, occupandosi però di regolare solo uno degli usi del captatore informatico, quale specifica modalità di intercettazione tra presenti, avente a oggetto solo i dispositivi mobili portatili.

Nel prosieguo si analizzerà il captatore informatico e la sua natura in quanto malware che consente numerose operazioni. L'articolo è così suddiviso: il paragrafo 2 approfondisce l'anatomia e l'inserimento dei malware, soffermandosi sui captatori informatici per i dispositivi mobili; il paragrafo 3 affronta gli aspetti di natura internazionale ed europea; il paragrafo 4 analizza il tema del cybercrime *in iure condito* e *de iure condendo*. Il paragrafo 5 è dedicato alle conclusioni.

2. I malware: l'anatomia, l'inserimento e i malware per i dispositivi mobili

I malware sono software che possono apportare modifiche indesiderate o danni ai sistemi informatici. Questo termine proviene dalla contrazione di due parole inglesi: *MALicious* e *softWARE*. I malware hanno svariate funzioni: possono sottrarre le informazioni desiderate sul sistema "vittima", danneggiarle o modificarle, ma possono anche rubare le credenziali degli utenti che utilizzano il sistema; il loro scopo è quello di non creare effetti visibili sui sistemi informatici attaccati, così da poter persistere il più a lungo possibile sul dispositivo e perseguire i propri scopi.

I malware entrano all'interno dei sistemi in diversi modi: possono trovarsi nell'allegato di un messaggio e-mail[5], all'interno di un file di una pendrive USB[6] o possono trovarsi nel corso della navigazione Internet sulle pagine web visitabili[7].

Per quanto ne esistano diverse tipologie, i malware agiscono tutti nello stesso modo, possedendo un unico modello strutturale, il quale percorre quattro fasi. Una prima fase, denominata "infezione", riguarda il momento in cui il malware si introduce all'interno del sistema informatico e si installa. In questa prima fase il malware adatta alle proprie necessità le impostazioni del sistema, in particolare quella di non essere rilevato.

La seconda fase è denominata "quiescenza". Il codice del virus resta all'interno della memoria del sistema, in attesa che venga raggiunto lo scopo per cui è stato inserito. Il malware resterà all'interno del computer, finché non verrà eliminato il codice o non verrà rimosso da un software anti-malware.

La terza fase è di "replicazione e propagazione". Questa fase riguarda solo i virus e i *worm*, per i quali, al determinarsi di certe condizioni, il malware si replica e decide i bersagli da infettare, propagandosi per colpire anche altri sistemi.

Infine, la quarta fase riguarda le "azioni malevole", che corrispondono al compimento degli scopi per i quali il malware è stato inserito come la distruzione del sistema o il furto dei dati. Qualora il malware non venisse rimosso, il software tornerebbe alla fase di quiescenza.

Quando un malware entra all'interno di un sistema ha necessariamente bisogno di essere attivato dall'utente-vittima; quest'ultimo dovrà aprire il file contente il codice malevolo. Per fare in modo che la vittima non se ne accorga i file contenenti il codice sono solitamente nascosti all'interno di un contenuto lecito con struttura interna modificata. La modifica avviene attraverso la manipolazione dell'*header*, ovvero dell'intestazione di un file, contente le informazioni da mandare al sistema operativo, tra cui un puntatore che indica la prima istruzione da eseguirsi all'attivazione del programma. Quando si ha l'infezione, il virus si accoda al codice originale e dilata il file spostando il puntatore verso il codice malevolo creandone anche un altro indirizzato al codice originale. Così facendo, all'apertura del file il sistema operativo eseguirà prima il contenuto illecito e poi quello lecito.

Una volta che il malware è penetrato e ha infettato il sistema inizia una fase di quiescenza, dove il software malevolo resta in memoria finché non viene attivato. In questo momento è quiescente ma vigile per evitare di essere rilevato da parte dell'utente o di un software anti-malware.

La maggior parte dei malware, restando in memoria, possono essere rilevati da un utente esperto tramite un'applicazione che visualizzi i processi in esecuzione nel sistema operativo, motivo per cui gli attaccanti danno al software un nome di un programma già esistente all'interno del sistema; così, anche se l'utente scoprisse l'esistenza del malware non saprebbe quali tra i due programmi – quello lecito e quello illecito – eliminare[8].

Come anticipato, i controlli possono essere svolti tanto da un utente esperto, quanto da un anti-malware. Gli attaccanti sviluppano il virus in modo tale da nasconderlo anche a un eventuale programma di sicurezza; le tecniche utilizzate per smascherare il virus vengono definite "statiche" o "dinamiche".

Nel primo caso, il malware potrebbe essere rilevato attraverso la ricerca del codice malevolo all'interno di file presenti sulla memoria o su flussi di dati tra-

smessi sulla rete. Ad ogni file viene attribuita una firma, basata su algoritmi di *hash*, che lo identifica in modo univoco e perde la sua validità se il file viene modificato. Il malware verrebbe rilevato attraverso un codice virale, anch'esso codificato con algoritmi di *hash*, chiamato *virus signature*. Il programma antivirus scansiona tutti i file e rileva corrispondenze errate tra i dati e le sequenze dei codici virali note. Questo metodo sarà valido per tutti i malware che sono conosciuti, mentre nulla varrà nei confronti di quei malware non ancora noti. I produttori dei programmi antivirus aggiornano continuamente i software da loro prodotti ma, per proteggere il sistema dal giorno in cui potrebbe essere rilasciato il malware "sconosciuto" a quello in cui verrà aggiornato il database, vengono utilizzate tecniche statiche che permettono il riconoscimento del codice malevolo senza avvalersi però del sistema delle firme. La tecnica in questione prevede che vengano raccolti dapprima i dati – i quali si riferiscono ad una particolare caratteristica virale, ad esempio, la presenza di un codice cifrato – poi, verranno analizzati tramite l'associazione ad un certo grado di pericolosità e sarà stilato un report che raccoglie le statistiche con riguardo al file oggetto di scansione. Ogni valore verrà aggiunto al report e il suo contenuto verrà valutato come pulito, sospetto o infetto. Questo tipo di tecnica statica si basa sull'euristica, per via della mancata conoscenza dei malware. è evidente come dapprima sia necessario effettuare dei tentativi utili per trovare eventuali virus.

Solitamente, per nascondersi dai controlli statici anti-malware gli attaccanti mascherano il codice malevolo, così da renderlo illeggibile e mutevole nel tempo; lo stesso verrà cifrato per non essere rilevato tramite firme predefinite. La cifratura del malware – tramite l'uso di un'apposita chiave, detta *stub* – comporta, prima, che lo stesso venga decifrato. La chiave *stub* cifra e decifra il codice malevolo[9]. Tale chiave non sarà statica ma muterà di volta in volta per rendere il codice cifrato sempre diverso.

Un'altra tecnica utilizzata è quella di comprimere il codice malevolo tramite l'uso di un algoritmo di compressione. Così facendo la vittima non verrà insospettita da un'occupazione anomala della memoria. La tecnica in esame è nota come "pacchettizzazione" e prevede l'inserimento nel codice di una sequenza di istruzioni per lo spacchettamento.

Gli anti-malware utilizzano anche tecniche dinamiche per rilevare i virus: attraverso le stesse viene rilevato il comportamento dei programmi in esecuzione. Il monitoraggio è un elemento dell'antivirus, residente nella RAM, che ricerca comportamenti sospetti. Se viene rilevata un'azione allarmante il software può bloccare l'operazione corrente oppure terminare il programma o, ancora, chiedere all'utente di scegliere l'azione da intraprendere.

I malware fino a ora richiamati operano a livello locale, infettando un sistema per volta. Ebbene, esistono anche tipologie di malware che hanno come obiettivo quello di infettare a livello distribuito; così facendo ogni sistema infettato entra a far parte di una *botnet* formata da dispostivi collegati a Internet e controllati da un'unica entità, il *botmaster*.

Una *botnet* può essere composta da milioni di sistemi – detti *bot* o zombie – che possiedono un *kernel*[10] per scambiare informazioni con uno o più server remoti. Per fare questo, sfruttano i servizi di chat connettendosi a un canale protetto da una password o da reti peer-to-peer attraverso le quali controllano e impartiscono gli ordini ai sistemi infetti.

Solitamente le *botnet* vengono utilizzate per compiere attacchi "distributed denial of service" – i DDoS mirano a compromettere il funzionamento del sistema informatico attraverso l'invio di numerosi messaggi fino a esaurirne le risorse – o campagne di spam, ossia mail pubblicitarie volte a reclamizzare un prodotto.

Di seguito verranno generalmente richiamati esempi di incidenti informatici dovuti alla presenza di diverse tipologie di malware. Un primo caso è rappresentato dai *ransomware*, ovvero una particolare tipologia di malware il cui obiettivo è impedire alla vittima di accedere al sistema informatico e utilizzarne i documenti. Secondo il *2016 Italian Cybersecurity Report* di CIS Sapienza si tratta di un fenomeno in crescita. Vi sono anche i *malware Eye Pyramid*. Questo tipo di malware si diffonde tramite l'e-mail e, una volta installato, accede ai documenti e alla casella di posta elettronica del sistema infetto. Inoltre, cattura i tasti che vengono digitati dalla vittima, permettendo di captare ogni tipo di informazione.

Alla luce di quanto detto, è evidente come i malware abbiano giocato un ruolo fondamentale nell'acquisizione della prova tramite le intercettazioni effettuate sui telefoni cellulari e sui computer. I malware – denominati dalla giurisprudenza "captatori informatici" – vengono inseriti all'interno dei dispositivi mobili per acquisire le comunicazioni tanto tra presenti – le c.d. intercettazioni ambientali – quanto qualunque altro tipo di conversazione telefonica o di messaggi tra il soggetto intercettato e i terzi.

I captatori informatici vengono inseriti all'interno dello smartphone, o dei tablet, potendo cancellare o rubare i dati sensibili e potendo accedere a tutte le informazioni presenti sui sistemi infettati effettuando, ad esempio, screenshot dello schermo e acquisendo i dati presenti nella memoria e qualunque tipo di informazione, quali numeri di telefono, appuntamenti condivisi, e-mail, messaggi e geolocalizzazioni.

Tra i maggiori sistemi operativi presenti sul mercato della telefonia mobile ci sono "Google Android" e "Apple iOS", accomunati da politiche di sicurezza volte a proteggere contro accessi fisici non autorizzati, cifratura dei contenuti personali dell'utente[11] etc.

Secondo le statistiche, la maggior parte delle minacce riguarda i sistemi "Google Android" mentre una minima parte interessa i sistemi iOS, ciò è dovuto alla tipologia di sistema operativo. Il primo, infatti, è un sistema open source in cui colui che utilizza il dispositivo ne ha un pieno controllo, mentre iOS si caratterizza per avere una piattaforma chiusa dove l'utente ha molte meno possibilità di personalizzazione; questo comporta che il modello di sicurezza tra i due sistemi sopra citati è completamente diverso. *Apple* controlla, tramite l'*App Store*, ogni applicazione presente sul telefono verificando che il codice realizzato dagli sviluppatori sia legittimo[12].

L'inserimento dei malware all'interno dei dispositivi mobili viene effettuato principalmente attraverso il Web o i c.d. market (negozi di applicazioni).

Attraverso il Web, il malware si diffonde tramite un *drive-by download*[13]. Così facendo, il programma malevolo si introduce in modo silente nel sistema vittima senza che sia necessaria alcuna autorizzazione da parte della vittima.

Nel caso di market invece, viene realizzata un'applicazione apparentemente legittima che invogli l'utente a scaricarla. Alcuni esempi riguardano giochi particolarmente conosciuti. La realizzazione di questo tipo di malware è il *repackaging*, tramite cui un utente malevolo modifica e personalizza l'applicazione inserendovi il codice virale. Una volta completato il processo di "decompilazione" si avrà un'applicazione identica a quella originale che però non avrà alcuna firma digitale perché compromessa durante il processo menzionato.

La firma sarà facilmente realizzabile tramite un certificato "auto firmato", attraverso un canale non ufficiale; da questo momento l'applicazione potrà essere distribuita tramite una fonte sconosciuta. Anche se, solitamente, le impostazioni del sistema operativo non permettono che vengano installati questi contenuti, tramite una modifica da parte dell'utente l'applicazione potrà trovare ingresso all'interno del computer.

3. Gli aspetti giuridici internazionali ed europei sui reati informatici

La protezione giuridica dei sistemi informatici ha catturato l'attenzione sia del diritto nazionale sia di quello internazionale ed europeo. Il Consiglio d'Europa ha redatto una Convenzione internazionale contro la criminalità del cyberspazio[14], attraverso una lista di reati informatici e l'invito rivolto agli Stati membri di adeguare le proprie legislazioni.

Il Comitato dei Ministri adottò il progetto e lo aprì alla firma degli Stati europei ed extraeuropei in occasione della conferenza sul cybercrime tenutasi il 23 novembre 2001 a Budapest[15].

Tale Convenzione ebbe un ruolo fondamentale per il contrasto alla criminalità informatica, influenzando le legislazioni degli Stati membri del Consiglio d'Europa, al fine di regolamentare una materia che, fino ad allora, era stata oggetto unicamente della legge del mercato[16].

L'obiettivo primario della Convenzione[17] era quello di introdurre un target minimo sulla tutela dei beni giuridici offesi dai reati informatici e uno comune di strategie di contrasto per tali delitti, perseguendo l'obiettivo di creare un'armonizzazione tra le norme di contrasto presenti nei vari ordinamenti, data la natura transfrontaliera che talvolta hanno tali tipi di illeciti. A ciascuno Stato restava ferma la possibilità di disciplinare in modo più restrittivo la materia in esame[18].

In ambito europeo, con il Trattato di Lisbona la criminalità informatica è stata inserita nell'art. 83 TFUE tra i fenomeni di criminalità considerati come particolarmente gravi e di natura transnazionale, su cui l'Unione europea ha competenza penale. Con la direttiva 2016/1148[19], detta direttiva NIS[20], l'Unione europea ha inteso intensificare la sensibilizzazione degli Stati membri alla sicurezza del cyberspazio avverso la commissione dei reati informatici, attraverso l'adozione di misure volte a tutelare la sicurezza delle reti e i sistemi informativi dell'Unione europea. Gli obiettivi individuati dalla direttiva ai quali deve adeguarsi l'ordinamento nazionale degli Stati membri sono: gli obblighi di una maggiore trasparenza delle reti informatiche, tanto a livello nazionale che sovranazionale e un maggiore radicamento delle misure di sicurezza nei diritti sanciti dalla Carta dei diritti fondamentali dell'UE, a garanzia della libertà di espressione, della tutela dei dati personali e della vita privata. Inoltre, deve essere garantito un libero accesso alle reti verso tutti i cittadini dell'Unione, così da evitare qualunque analfabetismo digitale[21].

Tra gli obiettivi vengono individuate delle priorità strategiche secondo le quali è necessario raggiungere una cyber-resilienza tramite l'abbattimento del crimine informatico; sviluppare una politica comune tra gli Stati membri di "cyber-difesa" congiuntamente alla Politica di sicurezza e di difesa comune; sviluppare risorse industriali e tecnologiche per la sicurezza informatica e, infine, adottare una politica internazionale dell'UE riguardo Internet basandosi sul rispetto dei valori fondamentali dell'Unione europea. L'ultimo obiettivo posto dalla direttiva del 2016 è

quello di condividere la responsabilità per garantire la sicurezza delle reti, dovuto dalla sempre maggiore dipendenza che si ha nei confronti delle tecnologie dell'informazione e alla maggiore vulnerabilità per via dell'impatto che le reti e i sistemi informativi hanno nella vita quotidiana.

La direttiva NIS è rivolta alla protezione europea dalle minacce cyber delle infrastrutture critiche. In particolare, lo scopo della direttiva è quello di garantire una tutela di base e comune, verso le informazioni, le reti e i sistemi, all'interno dell'Unione europea, per salvaguardare la continuità dei servizi strategici in ambito civile, sociale ed economico[22].

Sempre nell'alveo della strategia europea in materia di cybersicurezza, a giugno 2019 è entrato in vigore il Regolamento UE sulla cybersicurezza[23] definita come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[24]. Il Regolamento introduce un sistema europeo di certificazione e un nuovo mandato, più forte, per l'Agenzia dell'Unione europea per la cybersicurezza[25].

La strategia adottata dall'Unione europea si pone l'obiettivo di creare un cyberspazio resiliente, che sia aperto e sicuro e che porti a una maggiore fiducia da parte dei cittadini europei verso gli strumenti e i servizi digitali.

4. Il cybercrime: *in iure condito* e *de iure condendo*

Alla fine dell'800 due giovani avvocati di Boston, Samuel Warren e Louis Brandeis, partendo dallo *jus solitudinis* – ovvero *right to be let alone* – coniarono il termine giuridico privacy, riservatezza, con un saggio pubblicato nel dicembre del 1890 dalla Harvard Law Review[26].

La nozione originaria di privacy e riservatezza riproduceva lo schema del diritto alla proprietà privata che esclude gli altri, a meno che non siano legittimati a entrare. La rivoluzione digitale ha trasformato la nozione di sfera privata, riguardo alle informazioni trasmesse e ricevute, attraverso scambi sempre più immediati ma non sempre controllati.

A livello internazionale, l'art. 8 CEDU[27] afferma il diritto al rispetto della corrispondenza di ciascuno e la non ingerenza dell'autorità pubblica nell'esercizio di tale diritto. L'eccezione a tale affermazione è costituita dalla possibilità che sia la legge a prevedere un'ingerenza da parte dell'autorità pubblica per garantire la tutela e il rispetto della pubblica sicurezza, del benessere economico del paese, della difesa, dell'ordine e della prevenzione dei reati. Per proseguire nel panorama internazionale, l'art. 17 del Patto Internazionale relativo ai diritti civili e politici[28] del 1966 sostiene il divieto di interferenze nella vita privata e nella corrispondenza di ciascuno, ritenendo che sia la legge a dover tutelare tale diritto.

In ambito europeo, con la Direttiva 95/46/CE[29] venne introdotta la tutela delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Successivamente, con l'entrata in vigore della Carta dei diritti fondamentali dell'Unione europea – c.d. Carta di Nizza – si riconobbe espressamente il diritto alla protezione dei dati personali. In particolare, l'art. 7 della Carta di Nizza[30] afferma il diritto al rispetto della vita privata e di quella familiare estendendo tale diritto anche alla corrispondenza. Ancora, l'art. 8 riconosce espressamente il diritto alla protezione dei dati personali[31]. Con l'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR)[32] la direttiva 95/46/CE viene abrogata.

Il nuovo Regolamento raccoglie l'esperienza europea degli ultimi anni, con particolare riferimento agli approdi giurisprudenziali della Corte di Giustizia dell'Unione europea e, in particolare, alla progressiva trasformazione dell'orientamento delle istituzioni europee verso una normativa europea sulla libera circolazione dei dati personali più incentrata sulla tutela dei diritti fondamentali[33].

Nell'ordinamento italiano, il diritto alla riservatezza ha il suo primo referente nel complesso di principi ricavabili dall'art. 2 della Costituzione.

Il diritto alla riservatezza viene desunto dall'interpretazione data di alcune norme della Costituzione quali: l'art. 13 sulla libertà personale, l'art. 14 sull'inviolabilità del domicilio e l'art. 15 che garantisce il diritto all'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione. Al secondo comma dello stesso articolo si afferma come, su disposizione motivata dell'autorità giudiziaria possa essere limitato il diritto di cui al primo comma, con le garanzie stabilite dalla legge[34].

Il diritto alla riservatezza si afferma nella giurisprudenza italiana a partire dagli anni Settanta[35] per proseguire fino alla legge 31 dicembre 1996 n. 675[36], confluita nel Codice Privacy[37], poi modificato dal decreto legislativo n. 101/2018[38].

Da una sommaria disamina della normativa menzionata, si può notare come la riservatezza sia sempre stata uno dei diritti cardine, tanto a livello nazionale quanto a livello europeo e internazionale. La sua tutela incontra come unico limite un atto motivato dell'autorità giudiziaria per garantire il rispetto di un bene, come per esempio la pubblica sicurezza, anch'esso tutelato dal legislatore.

In caso di intercettazioni a scopo investigativo attraverso l'utilizzo di un "agente intrusore", il virus informatico, c.d. trojan[39], il diritto alla riservatezza rischierebbe quindi di essere leso. Difatti, la forza invasiva del trojan porterebbe a una compressione del diritto in questione, essendo quindi necessario un bilanciamento tra le esigenze investigative e i diritti fondamentali dell'individuo.

In un primo momento, l'utilizzo dei trojan consentiva quella che era stata definita "perquisizione on line o elettronica". In tal caso, ci si riferiva all'installazione da remoto di un programma inviato congiuntamente a messaggi e-mail o sms, di un captatore informatico in un computer o in uno smartphone[40]. Tramite questo strumento è possibile captare tutto il traffico telefonico o informatico in arrivo e in partenza dal computer o dal cellulare; le informazioni che si vogliono captare sono, per così dire, "infettate" dal malware e lo smartphone diventa un mezzo controllato dal soggetto terzo che ha introdotto il captatore. Può essere attivata la videocamera, carpendo così le immagini e può essere copiata la memoria e decifrato quello che viene digitato sulla tastiera. I dati raccolti potranno così essere trasmessi in tempo reale in un sistema informatico in uso alla polizia giudiziaria.

Il sistema descritto è altamente utile per le indagini, permettendo ad esempio, che venga intercettata una comunicazione telefonica intercorrente tra due soggetti e direttamente sui loro terminali senza attraversare una struttura centrale di commutazione. In questo modo, la comunicazione viene captata per mezzo di dati informatici in forma crittografata, potendo essere letti solo da chi possiede la chiave di decodifica.

Nell'era dello smartphone, il presupposto dell'utilizzo del telefono cellulare è che tale oggetto sia sempre con noi, accompagnandoci in ogni nostro movimento e in ogni luogo. Così facendo, il legame di "dipendenza" che si crea tra il cellulare e la persona intercettata permette il suo utilizzo ovunque, quale perfetto mezzo di intercettazione (anche della vita dei terzi, che entrano in contatto con il soggetto intercettato).

In un primo momento la giurisprudenza di legittimità dichiarò infondate le censure verso i procedimenti cautelari sia per questioni di rito, riguardanti la genericità dei motivi, che per le implicazioni della normativa speciale, riguardo alle intercettazioni nei procedimenti di criminalità organizzata. In particolare, la giurisprudenza affermò che la censura relativa a un difetto di motivazione riguardante la mancata specificazione che nei luoghi di privata dimora, sottoposti a intercettazione ambientale, si stesse svolgendo l'attività criminosa risultava infondata. L'infondatezza della censura era motivata dal fatto che le captazioni erano state disposte *ex* art. 13 d.l. 13 maggio 1991, n. 152, conv. con modificazioni in l. 12 luglio 1991, n. 203 che prescinde da tale requisito, poiché prevede che l'intercettazione di comunicazione tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 c.p. si stia svolgendo l'attività criminosa[41].

Di segno opposto un secondo orientamento interpretativo della giurisprudenza di legittimità che affrontò il tema del nuovo strumento investigativo attraverso una disamina delle peculiarità tecniche che contraddistinguevano tale modo di eseguire le intercettazioni: l'attivazione a distanza del microfono e quella della telecamera[42]. La Corte di Cassazione affermò che l'attivazione a distanza del microfono rappresentava un'intercettazione ambientale; la sua legittimità andava valutata alla luce dell'art. 266, comma secondo, c.p.p. e riguardava l'intercettazione di comunicazioni tra presenti in un luogo determinato. La norma doveva essere interpretata alla luce dell'art. 15 Cost. Il punto dolente era però rappresentato dalla possibilità che il soggetto si spostasse e il cellulare – attivo in qualità di microfono – captasse qualunque conversazione fatta dal soggetto intercettato con terzi, in una pluralità di luoghi diversi. Così facendo, la giurisprudenza di legittimità diede un'interpretazione costituzionalmente orientata propendendo per la tesi secondo cui le intercettazioni sono legittime solo nei luoghi specificati dal decreto autorizzativo, il quale dovrà individuare con precisione dove dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo legittimo quel provvedimento autorizzativo che indica in modo indeterminato i luoghi o, addirittura, non dà indicazioni a riguardo. Il secondo aspetto problematico riguardava l'attivazione a distanza della telecamera del telefono cellulare o del computer per effettuare le video riprese. Le video riprese non possono essere effettuate ovunque per evitare violazioni dell'art. 14 Cost. La tutela costituzionale del domicilio è riservata ai luoghi con i quali il soggetto ha un rapporto stabile; nel caso in cui le attività si svolgano in luoghi che non hanno natura di domicilio, le video riprese possono essere effettuate incontrando come unico limite la tutela alla riservatezza di cui all'art. 8 CEDU e dell'art. 2 Cost. Le prove così acquisite potranno essere utilizzate in qualità di prove atipiche in quanto ammesse con un provvedimento motivato dell'Autorità giudiziaria.

A tal fine, ad avviso della Corte, non saranno utilizzabili quelle riprese effettuate tramite l'uso dell'agente intrusore all'interno del domicilio e quelle compiute in ambienti in cui vada salvaguardata la riservatezza a meno che non vi sia un provvedimento dell'Autorità giudiziaria che specifichi le ragioni che inducono a compiere l'atto per la ricerca della

prova del reato. La Corte di Cassazione dà, quindi, un'interpretazione restrittiva escludendo che le intercettazioni ambientali tramite captatore informatico possano essere attuate ovunque si sposti il soggetto, essendo ritenute legittime soltanto qualora il decreto autorizzativo individui con precisione i luoghi in cui deve essere espletata l'attività captativa[43].

Nel 2016 si ha un importante punto di svolta sull'utilizzo dei captatori informatici per le intercettazioni ambientali. In particolare, la Corte di Cassazione[44] rimette alle Sezioni Unite la questione, formulando dei quesiti, così sintetizzabili: se nei luoghi di privata dimora *ex* art. 614 c.p., anche se non precisamente individuati e senza che si stia svolgendo l'attività criminosa, sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (come per esempio personal computer, tablet, smartphone)[45]. Le Sezioni Unite della Cassazione[46] rilevarono che per i reati di cui all'art. 51, comma 3-*bis* e comma 3-*quater* c.p.p., nonché comunque facenti capo a un'associazione per delinquere con esclusione del mero concorso di persone nel reato, l'uso del virus informatico è consentito anche nei luoghi di privata dimora, per realizzare intercettazioni "tra presenti", senza necessità che sia in atto l'attività criminosa e senza una preventiva individuazione degli stessi[47].

Al di fuori dell'ipotesi della commissione di reati di criminalità organizzata, la Corte rileva che si potrà comunque procedere all'uso di trojan, purché venga richiesto *ex ante* nel provvedimento di autorizzazione e vengano ribaditi i luoghi nei quali espletare l'attività di intercettazione della/e comunicazione/i determinando così quelle da escludere, fatta salva l'attività criminosa *in itinere*.

In attuazione dei criteri contenuti nell'art. 1, comma 84, lett. e), della legge n. 103 del 2017[48] è stato adottato il d.lgs. 29 dicembre 2017, n. 216[49], che, nell'ambito della riforma delle intercettazioni ha disciplinato l'utilizzo nelle indagini del captatore informatico[50]. Alcune delle modifiche più rilevanti riguardano, in particolare, l'art. 4 del d.lgs. 216/2017, che ha modificato il codice di procedura penale in materia di intercettazioni, mediante l'inserimento del captatore informatico, fissando i limiti di ammissibilità delle intercettazioni tra presenti. Difatti, è stato modificato l'art. 266, comma 2, c.p.p. inserendo la possibilità di eseguire le intercettazioni tra presenti anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora le intercettazioni avvengano nei luoghi di privata dimora è possibile eseguirle solo qualora vi sia fondato motivo di ritenere che in quei luoghi si stia svolgendo l'attività criminosa[51].

Inoltre, è stato inserito dall'art. 4 del decreto legislativo citato anche il comma 2-*bis* per il quale l'intercettazione di comunicazioni tra presenti mediante l'uso del trojan inserito su dispositivo elettronico portatile è sempre consentito nei procedimenti per i reati di criminalità organizzata, ovvero quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater*, c.p.p.[52]

Per quanto riguarda i presupposti e le forme del decreto che autorizza l'intercettazione tra presenti mediante l'utilizzo del captatore informatico, il nuovo art. 267 c.p.p. dispone che il giudice per le indagini preliminari debba autorizzare con decreto motivato quando vi siano gravi indizi di reato e l'intercettazione è considerata come assolutamente indispensabile ai fini della prosecuzione delle indagini. Inoltre, il decreto autorizzativo del gip dovrà essere adeguatamente motivato in merito alla scelta di ricorrere all'uso del captatore informatico per rilevare le conversazioni tra presenti. Al contempo, qualora si proceda per delitti diversi da quelli indicati dall'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e dei delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione, per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, il decreto autorizzativo dovrà indicare gli ambienti e il tempo in cui la stessa dovrà avvenire[53], «secondo un verosimile progetto investigativo che implica l'individuazione anche in forma indiretta dei luoghi in cui si sposterà il dispositivo mobile controllato, e sempre che si proceda "per delitti diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater*"»[54]. Ancora, qualora vi siano casi di urgenza e vi sia fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave per le indagini, il pubblico ministero procede con decreto motivato all'intercettazione tra presenti mediate l'inserimento del trojan su dispositivo elettronico portatile. Tale evenienza è possibile solo per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni. Inoltre, il pubblico ministero, oltre a indicare le ragioni che rendono necessaria tale scelta per lo svolgimento delle indagini, indica anche le ragioni dell'urgenza che non rendono possibile attendere il provvedimento del giudice[55].

La modifica stessa all'art. 267 c.p.p. mette in risalto come il ruolo svolto dal giudice per le indagini preliminari si faccia più intenso attraverso un'ingerenza diretta nelle indagini svolte dal pubblico ministero e una valutazione sull'utilità dello strumento investigativo richiesto da quest'ultimo[56].

Infine, sono state apportate delle modifiche anche in riferimento all'art. 270 c.p.p. sull'uso processuale

del materiale probatorio raccolto a seguito dell'intercettazione tra presenti operata con captatore informatico su dispositivo elettronico portatile. In particolare, al comma 1-*bis* dell'art. 270 c.p.p. si afferma che possono essere utilizzati i risultati delle intercettazioni tra presenti operate con trojan su dispositivo elettronico portatile anche per fornire la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione. Tale possibilità è ammessa qualora i risultati così acquisiti siano indispensabili per l'accertamento dei delitti indicati dall'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e dei delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione, per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.

Dall'analisi svolta si vuole evidenziare però come l'introduzione del d.lgs. 29 dicembre 2017, n. 216 abbia inteso regolare solo uno dei possibili usi dei captatori informatici, nello svolgimento delle attività investigative, attraverso l'inserimento del trojan all'interno di dispositivi elettronici portatili per effettuare intercettazioni tra presenti. Come visto infatti, il trojan ha una molteplicità di usi, tra cui la captazione dei dati in partenza e in arrivo su un dispositivo elettronico, l'acquisizione di comunicazioni e conversazioni avvenute mediante applicazioni di instant messaging, quali WhatsApp, Facebook messanger, Instagram, etc., l'attivazione del microfono o della telecamera, la possibilità di effettuare perquisizioni totali o parziali dell'hard disk, la possibilità di decifrare tutto ciò che viene digitato sul dispositivo bersaglio (la c.d. funzione *keylogger*[57]) e la possibilità di effettuare delle geolocalizzazioni.

Il captatore informatico è stato infatti definito un *congegno bulimico*[58] che da un remoto centro di comando carpisce tutte le informazioni necessarie acquisendole dal dispositivo bersaglio[59]. Nella prospettiva del cybercrime *de iure condendo* sarebbe auspicabile regolare gli usi – almeno quelli più comuni – del captatore informatico per eseguire le indagini, senza tralasciare la regolazione anche dell'inserimento del malware all'interno di dispositivi elettronici fissi, come per esempio le *smart tv*. In questo modo sarebbe possibile, da un lato avere una corretta qualificazione giuridica ogni qual volta il programma informatico venisse utilizzato mediante mezzi di ricerca della prova diversi dalle intercettazioni delle comunicazioni tra presenti, come, per esempio, le perquisizioni da remoto mediante virus trojan[60] e, dall'altro, la possibilità di ricercare una sempre maggiore tutela e un corretto bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati, previsto e tutelato dall'art. 112 Cost. relativo al principio dell'obbligatorietà dell'azione penale e, l'art. 15 Cost. che sancisce il principio di inviolabilità della riservatezza e segretezza di qualsiasi forma di comunicazione.

Dal punto di vista internazionale, a giudizio della Corte EDU, la compatibilità tra l'utilizzo dei captatori informatici nel corso dell'attività investigativa e la tutela del diritto alla riservatezza, di cui all'art. 8 CEDU, si basa sul rispetto di tre parametri fondamentali: la base giuridica appropriata, la finalità legittima e la necessità all'interno di una società democratica[61].

Nella sentenza *Zakharov c. Russia* del 2015, la Corte EDU precisa come non sia necessario indicare nel provvedimento autorizzativo delle intercettazioni i luoghi in cui le stesse debbano svolgersi, purché ne venga identificato il destinatario. Nell'utilizzo del trojan, il riferimento al luogo di svolgimento dell'intercettazione tra presenti non rappresenta il presupposto di autorizzabilità, necessario per il rispetto dell'art. 8 CEDU, secondo l'interpretazione data dalla giurisprudenza della Corte di Strasburgo. Difatti, è consentito, in via alternativa, far ricorso all'indicazione del destinatario dell'intercettazione tra presenti, anche in considerazione della natura dinamica e "itinerante" del mezzo utilizzato, che prescinde dal riferimento dei luoghi[62].

Dal punto di vista dell'ordinamento nazionale, affinché la Costituzione non sia violata è fondamentale constatare che vi sia il giusto bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati e il principio di inviolabilità della sfera di riservatezza e segretezza di qualsiasi forma di comunicazione[63].

La Corte costituzionale, nella sentenza n. 20 del 2017, ha evidenziato come i diritti di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione sono oggetto del diritto inviolabile tutelato dall'art. 15 Cost., che garantisce «quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana» (citando le sentenze n. 366 del 1991 e n. 81 del 1993). Inoltre, i giudici delle leggi sottolineano che, al pari di ogni altro diritto costituzionalmente protetto, anche il diritto alla libertà e alla segretezza della corrispondenza può essere soggetto a limitazioni, purché disposte «per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge», poiché, se così non fosse, «si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette» (sentenza n. 85 del 2013). Per questo, la «Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi», nel rispet-

to dei canoni di proporzionalità e di ragionevolezza (sentenza n. 85 del 2013). Pertanto, anche il diritto inviolabile protetto dall'art. 15 Cost. può subire limitazioni o restrizioni «in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia» della riserva assoluta di legge e della riserva di giurisdizione (sentenza n. 366 del 1991)[64].

5. Conclusioni

Alla luce di quanto detto, si è voluto analizzare brevemente come, da un lato, la natura stessa del captatore informatico gli impedisca di essere adeguatamente regolato dal legislatore nazionale e, dall'altro, ci sia una continua osmosi tra gli ordinamenti giuridici internazionali per combattere il cybercrime. La natura dinamica, itinerante e le specifiche modalità attuative dei captatori informatici, utilizzati a fini investigativi per la persecuzione di gravi reati, comporta la necessità di una costante valutazione circa l'opportunità di tale peculiare mezzo di ricerca della prova e il rispetto del diritto alla riservatezza.

Nei prossimi anni l'Italia dovrà porsi, quali sempre più rilevanti obiettivi strategici, l'abbattimento del crimine informatico e un adeguato sviluppo di risorse tecnologiche per la sicurezza informatica in grado di creare sistemi "cyber resilienti".

Se, in un caso l'obiettivo è quello di tutelare le reti, i sistemi e servizi informativi, nell'altro si è voluto evidenziare come i malware, con la loro peculiare struttura, rappresentano degli importanti strumenti investigativi per garantire la sicurezza nazionale che necessitano di una più specifica regolazione, pur nei limiti della natura tecnologica e, inevitabilmente, "itinerante" del mezzo. Tali mezzi di utilizzo del captatore informatico rappresentano le due facce della stessa medaglia e di come questo possa cambiare la loro natura da "malevola in benevola".

Note

[1]La nozione è stata sviluppata da Vittorio Frosini. A lui si devono le prime riflessioni generali sul rapporto tra informatica, diritto e attività giudiziarie. Frosini è considerato il padre del c.d. umanesimo tecnologico. Egli affermò che ci si trovava dinnanzi a una nuova democrazia di massa in cui si realizza una nuova forma di libertà individuale e un potenziamento della forza intellettuale e operativa del singolo individuo all'interno della comunità.V. Frosini, *La democrazia nel XXI secolo*, Liberilibri, 2010.

[2]A tal riguardo, la Corte di Cassazione si pronunciò circa la contestazione al ricorrente di aver sottratto dei file al detentore e che tale spossessamento fosse avvenuto attraverso la copiatura di detti file. In merito, la Corte osservava come l'art. 624 c.p. avesse quale presupposto necessario l'impossessamento della cosa mobile altrui, sottraendola a chi la detiene. Nella fattispecie trattata, la copiatura dei file presupponeva che gli stessi fossero rimasti all'interno del computer, o del CD, del detentore e che il presunto agente nel reato di furto fosse entrato in possesso di una copia, senza che la precedente situazione di fatto fosse modificata a danno del soggetto già possessore dei file. Così facendo la Suprema Corte, sulla base dell'assenza del *fumus commissi delicti*, rilevando il difetto di motivazione disponeva l'annullamento con rinvio del provvedimento impugnato per un nuovo esame sul punto. Cass. Penale, Sez. IV, 13 novembre 2003, n. 3449. Successivamente, la Suprema Corte affermò il principio per cui, nel caso di riproduzione non autorizzata di programmi aziendali e di notizie riservate tramite l'accesso a un sistema operativo aziendale sussistono gli estremi per la configurazione del concorso tra accesso abusivo a un sistema informatico o telematico – art. 615-*ter* c.p. – e la frode informatica (art. 640-*ter* c.p.). Cass. Penale, Sez. II, 4 maggio 2006, n. 30663.

[3]C. Sarzana di S. Ippolito, *Informazioni, internet e diritto penale*, III ed., Giuffré, 2010, 288 p.

[4]Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato, in CED Cass. n. 266905-266906.

[5]Quando l'inserimento avviene tramite posta elettronica il malware, allegato ad un messaggio, ha accesso più facile al sistema in quanto porta l'utente ad aprire il messaggio di posta con in allegato, ad esempio, un file di testo.

[6]Il supporto di memorizzazione – ad esempio, un'unità USB – serve a trasferire il malware nel sistema. Le modalità di trasporto e inserimento possono essere guidate tanto da colui che ha inserito il malware quanto dalla vittima, completamente inconsapevole. Questa modalità di inserimento del malware prevede, quindi, un accesso fisico al PC.

[7]Quando il malware viene inserito nel sistema informatico tramite il Web – in particolare, tramite un codice malevolo attraverso un download da una pagina Web – la vittima può svolgere sia un ruolo attivo sia passivo. Nel caso in cui svolga un ruolo attivo, l'utente contrae il malware scaricando un file, che appare "innocente" essendo in realtà malevolo. Nel secondo caso, invece, l'aggressore usa tecniche note come "drive-by download" che trasmettono un malware aprendo semplicemente una pagina Web. Con le misure di sicurezza assenti o compromesse, il malware attacca sulle vulnerabilità presenti nel browser evitando interazioni con l'utente-vittima.

[8]Talvolta, i malware assumono le sembianze di programmi essenziali per il funzionamento del sistema.

[9]Per quanto esistano diverse tecniche per la cifratura, quella più utilizzata sfrutta una chiave segreta secondo la crittografia simmetrica, ovvero l'utilizzo della stessa chiave sia per la crittazione che per la decrittazione.

[10]Il *kernel* è il nucleo di un sistema operativo. Il compito di questo software è quello di fornire un accesso sicuro all'hardware ai processi in esecuzione sull'elaboratore.

[11]M. Mezzalama, A. Lioy, H. Metwalley, *Anatomia del malware*, in "Mondo Digitale", n. 47, 2013.

[12]Google invece effettua controlli meno rigidi sugli sviluppatori e sulle applicazioni disponibili su Google Play; infatti, è possibile installare programmi esterni allo stesso.

[13]Il *drive-by download* si riferisce a due ambiti, entrambi riguardanti il download di un software da Internet: nel primo caso, ci si riferisce a quando l'utente accetta di scaricare un programma in modo automatico, nel secondo caso si fa riferimento al download che avviene senza che l'utente se ne accorga.

[14]Convenzione sulla criminalità informatica (STE n. 185), Budapest, 23 novembre 2001, entrata in vigore il 1º luglio 2004.

[15]L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Giappichelli, 2009.

[16]Prima della Convenzione, ogni riferimento ai reati informatici riguardava, tanto nel Common law quanto nel Civil law, "la legge del mercato". Per tale si intende ambiti nei quali far rientrare il diritto d'autore e le leggi sui segreti industriali e commerciali.

[17]In Italia la Convenzione fu oggetto di ratifica con la legge 18 marzo 2008, n. 48. Nel Codice penale italiano vennero introdotti nuovi reati quali: il falso informatico, il danneggiamento informatico, la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, etc. Allo stesso modo, vennero effettuate delle modifiche al Codice di procedura penale nella sezione dei mezzi di ricerca della prova e in quella riguardante le indagini della polizia giudiziaria, con il fine di indicare specifiche modalità di compimento delle stesse attraverso regole volte all'indicazione di come effettuare le ispezioni, perquisizioni e sequestri, senza ledere i dati originali e con la massima conformità della copia all'originale.

[18]F. Resta, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura*, in "Giurisprudenza di merito", 2008, n. 9, p. 2159.

[19]Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La direttiva (UE) 2016/1148 è stata recepita nell'ordinamento nazionale attraverso il decreto legislativo 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018. Il considerando (1) della direttiva afferma che «Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. è essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno». In tal senso, l'art. 1 della direttiva, nel delinearne l'oggetto e l'ambito di applicazione statuisce al par. 1 che «La presente direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno».

[20]*Network and Information Security Directive.*

[21]R. Scavizzi, *Ue: nuove misure di contrasto agli incidenti informatici e alla criminalità telematica*, in "Eurocomunicazione", 29 luglio 2016.

[22]La direttiva NIS identifica i soggetti da tutelare dividendoli in due categorie: gli OES - *Operators of Essential Services* e i DSP - *Digital Service Providers*. Saranno poi gli Stati membri a definire quali delle proprie organizzazioni inserire. La direttiva è stata recepita nell'ordinamento nazionale attraverso il d.lgs. 18 maggio 2018, n. 65, anche detto decreto legislativo NIS, entrato in vigore dal 24 giugno 2018. Subito dopo l'adozione del decreto legislativo NIS, la normativa italiana sulla cybersecurity è stata rafforzata attraverso l'istituzione del perimetro di sicurezza nazionale cibernetica e i relativi decreti attuativi. La direttiva NIS sarà comunque oggetto di aggiornamento in quanto verrà sostituita dalla direttiva NIS 2 che amplierà i soggetti da tutelare includendo anche: le pubbliche amministrazioni, i service provider pubblici di comunicazione elettronica, i provider di servizi digitali, i fornitori del trattamento delle acque reflue e la gestione dei rifiuti, gli operatori nella fabbricazione di prodotti essenziali, i servizi postali e di corriere e il settore sanitario. Per un maggiore approfondimento si veda L. Sbriz, *Direttiva NIS, ecco i vantaggi per le aziende nell'usarla come linea guida sulla sicurezza*, in "CyberSecurity.it", 2022; M. Santarelli, *Verso la NIS 2, c'è l'accordo in Europa: ecco le novità su soggetti coinvolti e obiettivi*, *ivi*, 2022; L. Tosoni, *Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto*, in "AgendaDigitale.eu", 2021.

[23]Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).

[24]*Ivi*, art. 2, 1).

[25]Per maggiori informazioni, si veda Consiglio europeo, *Cibersicurezza: la risposta dell'UE alle minacce informatiche*, novembre 2022.

[26]S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in "Harvard Law Review", 1890, n. 4, p. 193 ss.

[27]Diritto al rispetto della vita privata e familiare. «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

[28]Art. 17 Patto internazionale relativo ai diritti civili e politici «1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese».

[29]Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[30]Articolo 7 Carta dei diritti fondamentali dell'Unione Europea. *Rispetto della vita privata e della vita familiare* «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

[31]Articolo 8 Carta dei diritti fondamentali dell'Unione Europea, *Protezione dei dati di carattere personale* «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[32]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).

[33]M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in "Quaderni costituzionali", 2016, n. 3, p. 588.

[34]Sulla portata degli articoli 14 e 15 Cost. si veda P. Caretti, *I diritti fondamentali*, Giappichelli, 2011, p. 293. In particolare, si afferma che: «il diritto alla riservatezza viene definito come il diritto a mantenere riservato, salva espressa dichiarazione di volontà in senso contrario, quegli aspetti della propria vita privata, che attengono a fatti personalissimi che proprio per questo il soggetto ha il diritto di sottrarre alla conoscibilità dei terzi». Nel 1973 la Corte costituzionale in riferimento all'art. 15 Cost. ha affermato che «Questa norma non si limita a proclamare l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (comma primo), ma enuncia anche espressamente che "la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge" (comma secondo). Nel precetto costituzionale trovano perciò protezione due distinti interessi; quello inerente alla libertà ed alla segretezza

delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale». Corte Cost., 6 aprile 1973, n. 34, in "Consulta Online".

[35]A partire dalla sentenza del 27 maggio 1975, n. 2129, la Corte di Cassazione ha ritenuto definitivamente che l'ordinamento italiano riconoscesse il diritto alla riservatezza. La Corte affermava che il diritto in questione consisteva «nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze, che sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificate da interessi pubblici preminenti». Cass. Civ., Sez. I, 27 maggio 1975, n. 2129, in "Il Foro italiano", vol. 99, 1976, pp. 2895-2907. A titolo esemplificativo e non esaustivo si richiamano le successive pronunce della Corte di Cassazione che riconoscono quale *jus receptum* il diritto alla riservatezza: Cass., 5 aprile 1978, n.1557, in "Il Foro padano", I, 1979, p. 302; Cass. civ., Sez. III, 7 febbraio 1996, n. 982, in "Danno e responsabilità", 1996, p. 456; Cass., 7 febbraio 1996, n. 978, in "Corriere giuridico", 1996, n. 3, p. 264; Cass. Civ., Sez. III, 8 giugno 1998, n. 5658, in "Il Foro italiano", vol. 121, 1998, n. 9, pp. 2387-2394.

[36]L. 31 dicembre 1996 n. 675 (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*); legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali.

[37]D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

[38]D.lgs. 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).*

[39]In dottrina il tema è stato ampiamente trattato, *ex multis*: R. Flor, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in "Diritto Penale Contemporaneo", 2012, pp. 1-13; F. Iovene, *Le cd. perquisizioni on line: tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in "Diritto Penale Contemporaneo", 2014, n. 3-4, pp. 329-342; E. Lorenzetto, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, nota a Trib. Palermo, Sez. riesame, ord. 11 gennaio 2016, in "Diritto Penale Contemporaneo", 2016; L. Giordano, *Dopo le Sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, osservazioni a seguito di Cass., SSUU, sent. 28 aprile 2016, n. 26889, in "Diritto Penale Contemporaneo", 2017, n. 3, pp. 177-195.

[40]È importante sottolineare come i virus "spia" possano essere inseriti o all'interno di computer o all'interno di uno smartphone. Quando inseriti all'interno di uno smartphone assumono la veste o di un trojan come intercettatore ambientale – ovvero che capta comunicazioni tra presenti – o di un trojan come intercettatore telematico.

[41]Cass. Pen., Sez. VI, 8 aprile 2015, n. 27536; Cass. Pen., Sez. VI, 12 marzo 2015, n. 24237.

[42]Cass. Pen., Sez. VI, 26 maggio 2015, n. 27100, in CED Cass. n. 265654.

[43]P. Felicioni, *Le intercettazioni tra presenti mediante "captatore informatico" sono legittime nei procedimenti per delitti di criminalità organizzata*, in "Processo penale e giustizia", 2016, n. 5, pp. 118-138.

[44]Cass. Pen., Sez. VI, 10 marzo 2016, n. 13884.

[45]I quesiti sottoposti alle Sezioni Unite, con l'ordinanza n. 13884/16, cit. sono i seguenti: «se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione; se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. pen.; se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata».

[46]Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato, cit. Sui temi di cui si occupa la sentenza si v. A. Camon, *Cavalli di Troia in Cassazione*, in "Archivio della nuova procedura penale", 2017, n. 1, pp. 91-100; A. Balsamo, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in "Cass. pen.", 2016, pp. 2274-2288; G. Corasaniti, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in "Il Diritto dell'informazione e dell'informatica", 2016, p. 88; P. Felicioni, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in "Processo penale e giustizia", 2016, n. 5, p. 21; A. Gaito, S. Furfaro, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in "Archivio penale", 2016, n. 2, pp. 309-330; A. Cisterna, *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, *ivi*, pp. 331-347; L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, *ivi*, pp. 348-353; L. Picotti, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, *ivi*, pp. 354-365; L. Giordano, *Dopo le Sezioni unite sul "captatore informatico"*, cit.; G. Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in "Diritto Penale Contemporaneo", 7 ottobre 2016, p. 22.

[47]La Corte di Cassazione ha affermato che erano inutilizzabili i risultati acquisiti con il trojan soltanto per i procedimenti aventi ad oggetto reati comuni, limitando l'impiego del captatore informatico ai reati di criminalità organizzata. Il luogo dell'intercettazione sarà indifferente, ai sensi dell'art. 13 d.l. 13 maggio 1991, n. 152, convertito con modificazioni dalla l. 12 luglio 1991, n. 203. L. Giordano, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in "Diritto Penale Contemporaneo", 2017, n. 9, pp. 183-191.

[48]L. 23 giugno 2017, n. 103 *Modifiche al Codice penale, al codice di procedura penale e all'ordinamento penitenziario.* Entrata in vigore il 3 agosto 2017. Inoltre, l'art. 1, co. 84, lett. d), della legge n. 103 del 2017 ha delegato il Governo a adottare prescrizioni volte alla semplificazione «delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione». Per un maggiore approfondimento, si veda L. Giordano, *La delega per la riforma della disciplina delle intercettazioni*, in A. Marandola, T. Bene (a cura di), "La riforma della giustizia penale", Giuffré, 2017, pp. 382 ss.

[49]D.lgs. 29 dicembre 2017, n. 216, *Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103.* L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza*

"Scurato" alla riforma sulle intercettazioni, in "Diritto Penale Contemporaneo", 2018, n. 1, pp. 59-66. Il captatore informatico in materia di intercettazioni è oggetto della delega contenuta all'art. 1, co. 84, l. 23 giugno 2017, n. 103, c.d. *Riforma Orlando*. Nella Relazione illustrativa al d.lgs. 216/2017 si afferma che il delegante ha inteso regolare solo uno degli usi del captatore informatico, quale specifica modalità di intercettazione tra presenti, avente a oggetto solo i dispositivi mobili portatili. Difatti, a pagina 10 della Relazione illustrativa si evidenzia come il captatore informatico, consistendo in un malware, consente numerose operazioni, ma il delegante ha inteso limitare l'ambito applicativo dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inserimento del malware all'interno del dispositivo portatile, quali smartphone e tablet, e non anche di dispositivi fissi.

[50]Si veda G. Di Paolo, *Le intercettazioni mediante l'uso di captatore informatico*, in A. Giarda, F. Giunta, G. Varraso (a cura di), "Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura", Cedam-Wolters Kluwer, 2018, pp. 165 ss.; L. Giordano, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in "Sistema Penale", 2020, n. 4, pp. 109-143.

[51]Il comma 2, dell'art. 266 c.p.p. è stato modificato dall'art. 4, d.lgs. 216/2017 con decorrenza dal 26 gennaio 2018. Inoltre, quanto previsto dal comma 2, dell'art. 266 c.p.p. trovava applicazione alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019. Successivamente, il d.lgs. 216/2017, come modificato dalla l. 30 dicembre 2018, n. 145, ha disposto, con l'art. 9, comma 1, che le disposizioni degli artt. 2, 3 4, 5 e 7 si applicassero alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019.

[52]Inoltre, il comma 2-*bis* dell'art. 266 c.p.p. afferma che l'intercettazione di comunicazioni tra presenti mediante l'uso del trojan inserito su dispositivo elettronico portatile è consentita, previa indicazione delle ragioni che ne giustificano l'uso anche nei luoghi di privata dimora, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione.

[53]Il comma 1 è stato modificato dall'art. 2, co. 1, lett. d) del d.l. 30 dicembre 2019, n. 161, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7. Il d.l. 161/2019, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7, ha disposto, con l'art. 2, co. 8, che «Le disposizioni del presente articolo si applicano ai procedimenti penali iscritti successivamente al 30 aprile 2020».

[54]Cfr. p. 10 della Relazione illustrativa al d.lgs. 216/2017.

[55]Il comma 2-*bis* dell'art. 267 c.p.p. è stato inserito dall'art. 4, d.lgs. 216/2017 con decorrenza dal 26 gennaio 2018 e applicazione alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019. In un secondo momento, il d.lgs. 216/2017, come modificato dalla l. 30 dicembre 2018, n. 145, con l'art. 9, co. 1 ha disposto che «Le disposizioni di cui agli articoli 2, 3 4, 5 e 7 si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019». Tale comma è stato poi modificato dall'art. 2, co. 1, lett. d) del d.l. 161/2019, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7. Il d.l. 161/2019 ha poi disposto che le disposizioni dell'art. 2 si applicano ai procedimenti penali iscritti successivamente al 30 aprile 2020».

[56]La Suprema Corte ha precisato che «È tuttavia necessario, come stabilito nella citata pronuncia delle Sezioni Unite, il rispetto di un onere motivazionale rafforzato ai fini della emissione del provvedimento autorizzativo, poiché la forza intrusiva del mezzo usato ed il potenziale *vulnus* all'esercizio delle libertà costituzionalmente tutelate devono essere prudentemente bilanciati con il rispetto dei canoni di proporzione e ragionevolezza, cosicché la qualificazione, pure provvisoria, del fatto come inquadrabile in un contesto di criminalità organizzata risulti ancorata a sufficienti, sicuri ed obiettivi elementi indiziari che ne sorreggano, per un verso, la corretta formulazione da parte del Pubblico Ministero e, per altro verso, ne consentano la successiva, rigorosa, verifica dei presupposti da parte del Giudice chiamato ad autorizzare l'esecuzione delle relative operazioni di intercettazione». Cass., Sez. VI, sent. 13 giugno 2017, n. 36874. Per un maggiore approfondimento, la sentenza è stata commentata da L. Giordano, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in "Diritto Penale Contemporaneo", 2017, n. 9, pp. 183-191.

[57]In questo caso si è espressa la giurisprudenza di legittimità e, nel caso di specie, il virus trojan era stato utilizzato per acquisire delle password di accesso agli account di posta elettronica degli imputati. Ottenute queste password, gli inquirenti avevano potuto prendere visione sia dei messaggi che venivano inviati o ricevuti nella casella di posta elettronica che dei messaggi che venivano salvati nella cartella denominata bozze. La Suprema Corte ha ritenuto legittimo l'uso di un programma informatico per acquisire le credenziali di accesso alla casella di posta elettronica. Si veda Cass., Sez. IV, 28 giugno 2016, n. 40903, in CED Cass. n. 268228.

[58]L'espressione è stata coniata da L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in "ilpenalista.it", 2016.

[59]L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali*, cit., p. 60.

[60]Nel caso delle perquisizioni da remoto mediante virus trojan, la Corte costituzionale tedesca ha sottolineato quali siano i limiti giuridici dell'attività investigativa compiuta con mezzi di ricerca della prova che acquisiscano informazioni da remoto. Si veda *Bundersverfassungsgericht*, 27 febbraio 2008, in "Rivista trimestrale di diritto penale dell'economia", 2009, n. 3, p. 679. La Corte costituzionale tedesca, con la pronuncia appena citata ha dichiarato l'incostituzionalità delle disposizioni di legge che permettevano alla polizia federale, nei limiti del delitto di terrorismo internazionale, di ricorrere a misure di sorveglianza definite come occulte, tra cui la perquisizione da remoto. Sul punto si veda A. Balsamo, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in "Cassazione penale", 2016, n. 11, p. 4236. Per quanto riguarda la giurisprudenza nazionale si veda Cass., Sez. V, 14 ottobre 2009, n. 16556, in CED Cass. n. 246954 che è stata così massimata «È legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)».

[61]Corte EDU, Grande Camera, *Zakharov c. Russia*, ricorso n. 47143/06, 4 dicembre 2015, par. 227 ss.

[62]Cass., Sez. V, 30 settembre 2020, n. 35010.

[63]Nella sentenza 35010 del 2020 la Corte di Cassazione afferma che «sono, dunque, i mezzi di ricerca della prova a dover

essere coperti da riserva di legge, ma non le specifiche modalità attuative, influenzate da materiali questioni pratiche o di sviluppo tecnologico, a godere della medesima riserva, rimanendo evidente, peraltro, che l'unico profilo oggetto di verifica di costituzionalità sia quello relativo al fatto che "il legislatore abbia operato in concreto un bilanciamento tra il principio costituzionale della tutela della riservatezza nelle comunicazioni e l'interesse della collettività, anch'esso costituzionalmente protetto, alla repressione degli illeciti penali, senza imporre limitazioni irragionevoli o sproporzionate dell'uno o dell'altro (sentenza n. 372 del 2006)"». Cass., Sez. V, 30 settembre 2020 n. 35010.

[64]Cfr. punto 3.1. della sentenza della Corte costituzionale, n. 20 del 2017.

* * *

Profiles of the fight against cybercrime *in iure condito* and *de iure condendo*

Abstract: In the digital era, our lives are now inextricably linked to smartphones and tablets that follow us on our every move. It is precisely the itinerant nature of these media that makes them perfect 'containers' for hosting so-called cyber-captors, i.e., malware used for investigative purposes, for the prosecution of crimes. Thus, we examine how the case-law and the legislature have tried to rule on the advent of these new means of searching for evidence in an attempt to find a balance between satisfying the public interest in the investigation of crimes, provided for and protected by Article 112 of the Constitution on the principle of mandatory prosecution and Article 15 of the Constitution, which enshrines the principle of inviolability of confidentiality and secrecy of any form of communication. At the same time, however, it should be emphasized that the fight against cybercrime is essential, which is also implemented using such tools and an adequate development of technological resources for cyber security capable of creating systems that are 'cyber resilient'. In this sense, the dual nature, benevolent and malevolent, of the same means, malware, is brought to light.

Keywords: Malware – Cybersecurity – Cybercrime – Right to privacy – Cyber capturing

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0084

Osservatorio su
Intelligenza Artificiale e diritto
coordinato da Giancarlo Taddei Elmi

Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina

Giancarlo Taddei Elmi • Sofia Marchiafava

In linea con la Strategia europea, il 24 novembre 2021 l'Italia ha approvato il Programma strategico per l'Intelligenza Artificiale (IA) 2022-2024, nato dalla collaborazione tra Ministero dell'Università e della ricerca, Ministero dello Sviluppo economico e Ministero per l'Innovazione tecnologica e la transizione digitale.

In tale quadro questa rassegna si propone di costituire un primo strumento di conoscenza mirato per diffondere i principali recenti sviluppi della regolamentazione e giurisprudenza nazionale ed europea in materia di IA.

Sono riportati i più significativi atti europei e la giurisprudenza nazionale a partire dalla Risoluzione del Parlamento europeo P8_TA-PROV (2017) 0051, *Norme di diritto civile sulla robotica*, del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2013 (INL)).

Data la grande quantità di dottrina prodotta in tema di IA dal 2017, in questa rassegna, sono inseriti esclusivamente i contributi di commento e analisi dei testi normativi proposti in materia di IA, contenuti nella Risoluzione del Parlamento europeo del 20 ottobre 2020 (P9_TA(2020)0276) recante nell'allegato B) una proposta di Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, nella proposta di Regolamento del Parlamento europeo e del Consiglio europeo che stabilisce regole armonizzate sull'IA (Legge sull'IA) pubblicata dalla Commissione il 21 aprile 2021 (COM(2021) 206) e nella proposta per una direttiva del Parlamento e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale dell'intelligenza artificiale (Direttiva sulla responsabilità dell'IA), pubblicata dalla Commissione europea il 28 settembre 2022 (COM(2022) 496).

La rassegna è articolata in cinque sezioni rispettivamente dedicate a: (i) Unione europea e Intelligenza Artificiale; (ii) Il Consiglio d'Europa: Carta etica e raccomandazione; (iii) L'Italia e il Programma strategico nazionale per l'Intelligenza Artificiale; (iv) La giurisprudenza nazionale su Intelligenza Artificiale e diritto; (v) La dottrina su Intelligenza Artificiale e diritto limitatamente ai testi normativi proposti in materia di IA a partire dalla Risoluzione del Parlamento europeo del 20 ottobre 2020.

G. Taddei Elmi è ricercatore emerito CNR associato presso l'Istituto di informatica giuridica e sistemi giudiziari (IGSG) di Firenze e già docente di informatica giuridica presso le Università degli Studi di Firenze (Giurisprudenza e Scienze Politiche), di Milano (Cattolica e Statale) e di Cagliari, docente del Master di II livello in Informatica giuridica, nuove tecnologie e diritto dell'informatica (Dipartimento di Scienze Giuridiche, Sapienza - Università di Roma). S. Marchiafava è avvocato cassazionista, LLM in *Comparative Law*, docente del Master di II livello in Informatica giuridica, nuove tecnologie e diritto dell'informatica (Dipartimento di Scienze Giuridiche, Sapienza - Università di Roma).

1. Unione europea e intelligenza artificiale

1.1. La Commissione europea: comunicazioni e Libro bianco

Vengono riportati in ordine cronologico i principali atti e iniziative della Commissione europea in tema di IA.

2018

- *L'intelligenza artificiale per l'Europa, 25 aprile 2018, COM(2018) 237*
  In questa Comunicazione la Commissione europea ha annunciato la strategia europea per l'IA. Dopo una prima definizione ufficiale di IA sono indicate le priorità e iniziative da intraprendere, tra cui quella di «assicurare un quadro etico e giuridico adeguato» fondato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali.
- *Piano coordinato sull'intelligenza artificiale, 7 dicembre 2018 COM(2018) 795*
  Il piano coordinato sull'IA "made in Europe", fondato sulla dichiarazione di cooperazione firmata il 10 aprile 2018 da 24 Stati membri (tra cui l'Italia) e dalla Norvegia, rappresenta un quadro decisivo di riferimento per le strategie nazionali in tema di intelligenza artificiale. L'obiettivo primario è quello di favorire sinergie, condividere dati, e aumentare gli investimenti congiunti e progetti di ricerca comuni sull'IA.

2019

- *Creare fiducia nell'intelligenza artificiale antropocentrica, 8 aprile 2019, COM(2019) 168*
  Nella prospettiva europea l'IA e le sue applicazioni dovrebbero essere sviluppate secondo un approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali. In questa Comunicazione, la Commissione europea si sofferma anche sui sette requisiti che il suo Gruppo indipendente di esperti ad alto livello sull'IA ha individuato per stabilire l'affidabilità delle applicazioni di intelligenza artificiale: (i) intervento e sorveglianza umani, (ii) robustezza tecnica e sicurezza, (iii) riservatezza e governance dei dati, (iv) trasparenza, (v) diversità, non discriminazione ed equità, (vi) benessere sociale e ambientale, (vii) accountability.

2020

- *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, 19 febbraio 2020, COM(2020) 65*
  Nel Libro bianco la Commissione europea ribadisce i benefici sociali ed economici dell'IA, conferma l'esigenza di creare un contesto di fiducia e, quindi, uno sviluppo sicuro e affidabile dell'IA, rispettoso dei valori e dei diritti dei cittadini europei, in particolare di quelli sanciti nella Carta dei diritti fondamentali dell'UE. L'IA è, infatti, considerata una tecnologia strategica «a condizione che segua un approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali». In tale contesto si rende indispensabile incrementare la ricerca, la formazione, l'innovazione creando reti e centri europei nonché aumentare gli investimenti pubblici e privati sull'IA per il conseguimento di un «ecosistema di eccellenza». Il quadro normativo europeo deve essere adeguato anche per evitare la frammentazione del mercato interno che comprometterebbe gli obiettivi di fiducia e certezza del diritto.
- *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità, 19 febbraio 2020, COM(2020) 64*
  Nella relazione che accompagna il Libro bianco sono precisate in dettaglio le implicazioni in tema di sicurezza e responsabilità dell'IA nonché di altre tecnologie di seconda generazione (IoT e Robotica), la relativa normativa esistente e le possibili lacune.

1.2. Il Parlamento europeo: le risoluzioni

Sono riportate le risoluzioni e le iniziative in tema di IA e robotica del Parlamento europeo che, com'è noto, insieme ai rappresentanti dei governi dell'UE riuniti nel Consiglio, è responsabile dell'adozione della legislazione eurounionale.

2017

- *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, 16 febbraio 2017, P8_ TA(2017)0051*
  Preceduta dalla relazione della Commissione giuridica del Parlamento europeo (*Rapporto Delvaux*) questa risoluzione del Parlamento europeo pone l'attenzione su alcune fondamentali questioni della robotica e dell'IA, quali la crescente autonomia tecnologica raggiunta dai robot e i rischi connessi, le problematiche legate alla responsabilità civile in relazione alle azioni di robot sempre più autonomi e la possibilità di riconoscere lo status giuridico specifico di persona elettronica ai robot più sofisticati.

2018

- *Sui sistemi d'arma autonomi, 12 settembre 2018, P8_ TA(2018)0341*
  Per «sistemi d'arma autonomi letali» si intendono quei sistemi «privi di un controllo umano significativo sulle funzioni critiche della selezione e dell'attacco di bersagli individuali». In questa specifica risoluzione il Parlamento europeo ha espresso la necessità di impedirne lo sviluppo evidenziandone i rischi e ricordando la lettera aperta inviata nell'agosto 2017 alle Nazioni Unite da 116 fondatori di importanti imprese internazionali del settore della robotica e dell'intelligenza artificiale per invitare i governi a prevenire una corsa agli armamenti in relazione a tali armi e ad evitare gli effetti destabilizzanti di queste tecnologie.

2019

- *Su una politica industriale europea globale in materia di robotica e intelligenza artificiale, 12 febbraio 2019, P8_ TA(2019)0081*
  Dopo avere ricordato il crescente progresso nel settore dell'IA nonché la notevole diffusione delle sue applicazioni in tutti i settori, il Parlamento europeo, ha rilevato una duplice esigenza: quella di un quadro normativo adeguatamente flessibile per non ostacolare «l'innovazione e lo sviluppo libero di nuove tecnologie e nuovi impieghi dell'intelligenza artificiale» nonché quella «di politiche chiare in tutte le fasi di sviluppo» per evitare rischi ed eventuali effetti negativi. Inoltre, il Parlamento europeo ha esortato gli Stati membri a istituire partenariati tra industria, istituti di ricerca e centri di eccellenza comuni sottolineando che la ricerca nel campo dell'IA dovrebbe riguardare anche gli aspetti sociali, etici e di responsabilità civile ad essa correlati.

2020

- *Sui processi decisionali automatizzati: garantire la tutela dei consumatori e la libera circolazione di beni e servizi, 12 febbraio 2020, P9_ TA(2020)0032*
  Tenuto conto dei rischi connessi a prodotti con capacità decisionali autonome, il Parlamento europeo ha sottolineato in questa Risoluzione la necessità di tutelare i consumatori fornendo loro una adeguata informazione sul funzionamento e controllo dei sistemi decisionali automatizzati nonché sulla possibilità di rettificarne la decisione. Gli algoritmi devono essere spiegabili e imparziali, va assicurata la revisione per correggere eventuali errori nelle decisioni automatizzate, in ogni caso «gli esseri umani devono sempre essere responsabili».
- *Raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, 20 ottobre 2020, P9_ TA(2020)0275*
  Il Parlamento europeo ha sottolineato l'asimmetria tra coloro che impiegano le tecnologie di IA e coloro che ad esse sono assoggettati evidenziando la necessità di regole che stabiliscano una impostazione etica predefinita fin dalla progettazione dei sistemi di IA, la possibilità di un controllo e intervento umano. Nel confermare, tra l'altro, l'approccio del rischio il Parlamento europeo ha allegato alla sua risoluzione il testo di una proposta di regolamento sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate.
- *Raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 20 ottobre 2020, P9_ TA-PROV(2020)0276*
  Questa Risoluzione rappresenta una tappa fondamentale nell'elaborazione della annunciata normativa europea in materia di responsabilità civile per l'IA. Il modello normativo proposto, conforme alle indicazioni della Commissione europea, suddivide i sistemi di IA tra quelli che operano ad alto rischio oppure a basso

rischio, proponendo per i primi un regime comune di responsabilità oggettiva, mentre per gli altri un regime di responsabilità per colpa. Il criterio distintivo per stabilire il regime di responsabilità, oggettiva o per colpa, applicabile è il livello del rischio connesso ai sistemi di IA, stabilito a priori e in relazione ad alcuni fattori. Il Parlamento europeo ha allegato alla sua risoluzione il testo di una proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale.

- *Diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, 20 ottobre 2020, P9_ TA(2020)0277*
  Come osservato dal Parlamento europeo l'autonomizzazione del processo creativo di generazione di contenuti di carattere artistico può sollevare delle questioni in ordine alla titolarità dei diritti di proprietà intellettuale, ma si esclude la possibilità di riconoscere la personalità giuridica ai sistemi di IA evidenziando in ogni caso la differenza tra le creazioni umane ottenute con l'assistenza dell'IA e quelle autonomamente realizzate dall'IA.

2021

- *Intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale, 20 gennaio 2021, P9_ TA-PROV(2021)0009*
  La Risoluzione sottolinea alcuni aspetti e implicazioni dell'IA in relazione agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale. In proposito si sottolinea che se l'IA è impiegata in un contesto militare, gli Stati membri, le parti del conflitto e i singoli devono in ogni caso osservare i rispettivi obblighi previsti dal diritto internazionale applicabile e assumersi le relative responsabilità conseguenti all'uso di tali sistemi. Quando l'IA è utilizzata nella pubblica amministrazione va garantita «la spiegabilità degli algoritmi, la trasparenza e la sorveglianza regolamentare» e sono necessarie delle preventive valutazioni d'impatto. Inoltre, non è mai consentita la violazione dei diritti fondamentali nonché dei principi democratici e dello Stato di diritto.

2022

- *L'intelligenza artificiale in un'era digitale, 3 maggio 2022, P9_ TA(2022)0140*
  La Risoluzione è stata preceduta dalla relazione della Commissione speciale sull'intelligenza artificiale in un'era digitale del 5 aprile 2022 (A9-0088/2022) nella quale tra l'altro è stata precisata la tabella di marcia per consentire all'Unione europea di acquisire un ruolo centrale a livello mondiale nel settore dell'IA e recuperare il ritardo. I punti principali di questo programma prevedono: (i) un quadro normativo proporzionato al rischio, rispettoso dei valori e principi fondamentali europei, attento alla tutela dei soggetti più deboli (minori e consumatori); (ii) il completamento del mercato unico digitale, in particolare attraverso una revisione delle strategie nazionali per l'IA e l'eliminazione delle barriere; (iii) una infrastruttura efficace e veloce per l'IA, in linea con le esigenze ambientali; (iv) un quadro di competenze in materia di IA, caratterizzato da parità di genere e impulso alla ricerca; (v) una strategia industriale precisa e favorita da investimenti pubblici; (vi) la sicurezza, in particolare con riguardo alla cybersicurezza.
  La risoluzione del Parlamento europeo riprende la suddetta relazione indicando i molteplici aspetti della trasformazione digitale e dell'IA. Nel rilevare il ritardo dell'Unione europea rispetto agli USA e alla Cina, il Parlamento europeo sollecita azioni dirette ad assicurare un ruolo primario nell'elaborazione di un quadro normativo a livello internazionale sull'IA che tenga conto dei rischi e della necessità di rafforzare la cooperazione internazionale tra chi condivide gli stessi valori al fine di tutelare i diritti fondamentali e limitare le nuove minacce tecnologiche.

1.3. La normativa europea in itinere

2020

- Proposta ex art. 255 TFUE di *Regolamento sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate*
  (il testo della proposta è allegato 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))
  Il proposto regolamento intende «istituire un quadro normativo dell'Unione di principi etici e obblighi giuridici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate nell'Unione». Per le tecnologie ad alto rischio sono previsti molteplici e specifici obblighi.

- Proposta ex art. 255 TFUE di *Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*
  (il testo della proposta è allegato 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))
  La proposta delinea un modello normativo di regime di responsabilità civile fondato sulla suddivisione dei sistemi di IA tra quelli che operano ad alto rischio e quelli che operano a basso rischio, proponendo per i primi un regime comune di responsabilità oggettiva, mentre per gli altri un regime di responsabilità per colpa.

2021

- 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*, 21 aprile 2021, COM(2021) 206
  Questa proposta di Regolamento (anche denominato *Artificial Intelligence Act*) stabilisce regole armonizzate sull'IA, in particolare riguardo allo sviluppo, all'immissione sul mercato dell'UE, all'utilizzo di prodotti e servizi che ricorrono all'IA. La proposta fornisce una definizione e classificazione dei sistemi di IA, indica i requisiti obbligatori comuni per la loro progettazione e realizzazione, commercializzazione e utilizzo, prevede diversi strumenti di controllo e delle sanzioni. In particolare, secondo la proposta, i sistemi di IA utilizzati nell'UE sono classificati in base al rischio e a parametri ben delineati che tengono conto anche delle indicazioni contenute nel Libro bianco del 2020. Si individuano le seguenti categorie di rischio derivanti dall'uso dei sistemi di IA: inaccettabile, alto, basso, minimo.

2022

- Proposta per una *direttiva del Parlamento e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale dell'intelligenza artificiale (Direttiva sulla responsabilità dell'IA)*, 28 settembre 2022, COM(2022) 496
  La Commissione europea, facendo seguito alla Risoluzione del Parlamento europeo del 20 ottobre 2020, ha pubblicato una proposta di direttiva in materia di responsabilità extracontrattuale per i danni arrecati dai sistemi di IA di qualsiasi tipo (ad alto o basso rischio). La proposta di direttiva prevede una nuova disciplina da applicare ai soli giudizi civili promossi davanti ai giudici nazionali in caso di colpa extracontrattuale, quale inosservanza della diligenza dovuta, imputabile a chiunque (fornitori, sviluppatori, utenti), per il risarcimento di qualsiasi tipo di danno previsto dalla legge nazionale (vita, salute, proprietà, privacy, ecc.) e per qualsiasi tipo di soggetto danneggiato (persone fisiche, giuridiche).
  Il regime giuridico delineato da tale proposta richiama il quadro definitorio della *Legge sull'intelligenza artificiale* (art. 2) e dopo aver definito il "dovere di diligenza" (art. 2, n. 9) lascia agli ordinamenti giuridici dei rispettivi Stati membri di stabilire la nozione di "colpa" o "danno". Tale proposta detta regole comuni in tema di prova, in particolare in relazione all'esibizione dei mezzi istruttori riguardo ai sistemi di IA ad alto rischio (art. 1, lett. a) nonché sull'onere della prova (art. 1, lett. b).
  In relazione a tale disciplina gli Stati membri possono adottare o mantenere normative nazionali più favorevoli purché siano compatibili con il diritto dell'Unione europea (art. 1, n. 4).
  La proposta prevede due principali rimedi sul piano processuale in favore di coloro che sono danneggiati dai sistemi di IA e agiscono in sede civile: 1) il diritto dell'attore di chiedere al giudice un ordine di esibizione nei confronti del convenuto riguardo a informazioni e documenti sul sistema di IA ad alto rischio oggetto della pretesa risarcitoria (art. 3); 2) la "presunzione del nesso di causalità" tra la colpa del convenuto e il danno qualora sia dimostrata l'inosservanza di un determinato dovere legale o giudiziale e ne sia dimostrata la rilevanza ai fini della produzione del danno stesso (art. 4). Tale presunzione può subire delle limitazioni, in particolare nel caso in cui il convenuto dimostri la possibilità per l'attore di ottenere senza particolari difficoltà una relazione tecnica o elementi di prova. Inoltre, tale presunzione può applicarsi ai sistemi di IA a basso rischio solo laddove sia sussistente una effettiva difficoltà di carattere probatorio in capo all'attore (art. 4, n. 5). In ogni caso è ammessa la prova liberatoria e tale presunzione a carico del convenuto può essere rovesciata (art. 4, n. 7).

Un riesame dell'applicazione della direttiva da parte della Commissione europea è previsto al termine di cinque anni al fine di presentare una relazione al Parlamento europeo e al Consiglio nonché al Comitato economico e sociale europeo (art. 5).
La proposta di direttiva integra il quadro delineato dalla proposta di regolamento del 21 aprile 2021. Il rapporto tra le due proposte è sintetizzato chiaramente nella relazione che accompagna la proposta: trattasi di discipline applicabili in momenti diversi, rispettivamente prima e dopo il verificarsi dell'eventuale danno; sicurezza e responsabilità sono due facce della stessa medaglia. Come evidenziato nella stessa relazione, l'approccio della proposta direttiva è "graduale" in quanto tale proposta indica solo alcune regole, in particolare sotto il profilo probatorio per agevolare il danneggiato. Inoltre, sempre secondo tale approccio "graduale", si preferisce al regolamento la direttiva in quanto quest'ultima richiede un intervento normativo di recepimento da parte degli Stati membri.
Si riporta qui di seguito uno stralcio (artt. 1-4) del testo della proposta.

Articolo 1
Oggetto e ambito di applicazione

1. La presente direttiva stabilisce norme comuni per quanto riguarda:
   (a) la divulgazione di elementi di prova relativi a sistemi di intelligenza artificiale (IA) ad alto rischio per consentire all'attore in un'azione civile di responsabilità extracontrattuale per colpa di motivare adeguatamente la domanda di risarcimento del danno;
   (b) l'onere della prova nel quadro delle azioni civili di responsabilità extracontrattuale per colpa avviate dinanzi agli organi giurisdizionali nazionali per ottenere il risarcimento del danno causato da un sistema di IA.

2. La presente direttiva si applica alle azioni civili di responsabilità extracontrattuale per colpa volte a ottenere il risarcimento del danno causato da un sistema di IA dopo [*la fine del periodo di recepimento*].
   La presente direttiva non si applica alla responsabilità penale.

3. La presente direttiva non pregiudica:
   (a) le norme del diritto dell'Unione che disciplinano i criteri di responsabilità nel settore dei trasporti;
   (b) i diritti che le norme nazionali di attuazione della direttiva 85/374/CEE possono riconoscere al danneggiato;
   (c) le esenzioni dalla responsabilità e gli obblighi in materia di dovere di diligenza stabiliti dalla [legge sui servizi digitali] e
   (d) le norme nazionali che stabiliscono a quale parte incombe l'onere della prova e qual è il grado di certezza richiesto in relazione al livello della prova o che definiscono il concetto di colpa, tranne in relazione a quanto previsto agli articoli 3 e 4.

4. Gli Stati membri possono adottare o mantenere in vigore norme nazionali più favorevoli all'attore in relazione all'esigenza di motivare una domanda presentata nel quadro di un'azione civile di responsabilità extracontrattuale per ottenere il risarcimento del danno causato da un sistema di IA, a condizione che tali norme siano compatibili con il diritto dell'Unione.

Articolo 2
Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

(1) "sistema di IA": un sistema di IA quale definito [all'articolo 3, punto 1, della legge sull'IA];
(2) "sistema di IA ad alto rischio": un sistema di IA di cui [all'articolo 6 della legge sull'IA];
(3) "fornitore": un fornitore quale definito [all'articolo 3, punto 2, della legge sull'IA];
(4) "utente": un utente quale definito [all'articolo 3, punto 4, della legge sull'IA];
(5) "domanda di risarcimento del danno": una domanda nel quadro di un'azione civile di responsabilità extracontrattuale per colpa volta a ottenere il risarcimento del danno causato dall'output di un sistema di IA o dalla mancata produzione di un output che avrebbe invece dovuto essere prodotto da tale sistema;

(6) "attore": la persona che presenta una domanda di risarcimento del danno e che:
  (a) è stata danneggiata dall'output di un sistema di IA o dalla mancata produzione di un output che avrebbe invece dovuto essere prodotto da tale sistema;
  (b) è subentrata o si è surrogata nei diritti del danneggiato per legge o disposizione contrattuale; oppure
  (c) agisce per conto di uno o più danneggiati conformemente al diritto dell'Unione o nazionale;
(7) "attore potenziale": una persona fisica o giuridica che sta valutando la possibilità di presentare una domanda di risarcimento del danno, senza averla ancora presentata;
(8) "convenuto": la persona contro la quale è stata presentata una domanda di risarcimento del danno;
(9) "obbligo di diligenza": il livello di condotta richiesto, stabilito dal diritto nazionale o dell'Unione, al fine di evitare danni agli interessi giuridici riconosciuti dal diritto nazionale o dell'Unione, tra cui la vita, l'integrità fisica, la proprietà e la tutela dei diritti fondamentali.

Articolo 3
Divulgazione degli elementi di prova e presunzione relativa di non conformità

1. Gli Stati membri provvedono affinché, su richiesta di un attore potenziale che, dopo aver chiesto al fornitore, a una persona soggetta agli obblighi del fornitore a norma [dell'articolo 24 o dell'articolo 28, paragrafo 1, della legge sull'IA] o a un utente di divulgare gli elementi di prova pertinenti di cui dispone in relazione a un determinato sistema di IA ad alto rischio che si sospetta abbia cagionato il danno, si sia visto opporre un rifiuto, oppure su richiesta dell'attore, gli organi giurisdizionali nazionali abbiano il potere di ordinare la divulgazione di detti elementi di prova da parte di tali persone.
   L'attore potenziale deve presentare a sostegno di tale richiesta fatti e prove sufficienti a sostenere la plausibilità della domanda di risarcimento del danno.

2. Nel quadro di una domanda di risarcimento del danno, gli organi giurisdizionali nazionali ordinano a una delle persone elencate al paragrafo 1 di divulgare gli elementi di prova solo se l'attore ha previamente compiuto ogni sforzo proporzionato per ottenere tali elementi di prova dal convenuto.

3. Gli Stati membri provvedono affinché gli organi giurisdizionali nazionali, su richiesta dell'attore, abbiano il potere di ordinare misure specifiche di conservazione degli elementi di prova di cui al paragrafo 1.

4. Gli organi giurisdizionali nazionali limitano la divulgazione degli elementi di prova a quanto necessario e proporzionato per sostenere una domanda o potenziale domanda di risarcimento del danno e limitano la conservazione di tali elementi di prova a quanto necessario e proporzionato per sostenere tale domanda di risarcimento del danno.
   Nel valutare la proporzionalità di un ordine di divulgazione o di conservazione degli elementi di prova, gli organi giurisdizionali nazionali tengono conto dei legittimi interessi di tutte le parti, compresi i terzi interessati, specialmente in relazione alla protezione dei segreti commerciali ai sensi dell'articolo 2, punto 1, della direttiva (UE) 2016/943, e delle informazioni riservate, come le informazioni relative alla sicurezza pubblica o nazionale.
   Gli Stati membri provvedono affinché, qualora sia ordinata la divulgazione di un segreto commerciale o presunto segreto commerciale che l'organo giurisdizionale ha indicato come riservato ai sensi dell'articolo 9, paragrafo 1, della direttiva (UE) 2016/943, gli organi giurisdizionali nazionali, d'ufficio o su richiesta debitamente motivata di una parte, abbiano il potere di adottare misure specifiche necessarie per tutelarne la riservatezza se tali elementi di prova vengono utilizzati o se ad essi è fatto riferimento nel procedimento giudiziario.
   Gli Stati membri provvedono inoltre affinché la persona cui è stato ordinato di divulgare o conservare gli elementi di prova di cui al paragrafo 1 o 2 disponga di adeguati mezzi procedurali per impugnare tali ordinanze.

5. Se il convenuto non si conforma all'ordinanza con cui l'organo giurisdizionale nazionale, nel contesto di una domanda di risarcimento del danno, gli ingiunge di divulgare o conservare gli elementi di prova a sua disposizione a norma del paragrafo 1 o 2, l'organo giurisdizionale nazionale presume, in particolare nelle circostanze di cui all'articolo 4, paragrafo 2 o 3, la non conformità a un pertinente obbligo di diligenza da

parte del convenuto, che gli elementi di prova richiesti erano intesi a dimostrare ai fini della domanda di risarcimento del danno.
Il convenuto ha il diritto di confutare tale presunzione.

Articolo 4
Presunzione relativa del nesso di causalità in caso di colpa

1. Fatti salvi i requisiti di cui al presente articolo, ai fini dell'applicazione delle norme in materia di responsabilità alle domande di risarcimento del danno gli organi giurisdizionali nazionali presumono l'esistenza del nesso di causalità tra la colpa del convenuto e l'output prodotto da un sistema di IA o la mancata produzione di un output da parte di tale sistema se sono soddisfatte tutte le condizioni seguenti:
   (a) l'attore ha dimostrato o l'organo giurisdizionale ha presunto, a norma dell'articolo 3, paragrafo 5, la colpa del convenuto o di una persona della cui condotta il convenuto è responsabile, consistente nella non conformità a un obbligo di diligenza previsto dal diritto dell'Unione o nazionale e direttamente inteso a proteggere dal danno verificatosi;
   (b) si può ritenere ragionevolmente probabile, sulla base delle circostanze del caso, che il comportamento colposo abbia influito sull'output prodotto dal sistema di IA o sulla mancata produzione di un output da parte di tale sistema;
   (c) l'attore ha dimostrato che il danno è stato causato dall'output prodotto dal sistema di IA o dalla mancata produzione di un output da parte di tale sistema.

2. In caso di domanda di risarcimento del danno presentata contro un fornitore di un sistema di IA ad alto rischio soggetto ai requisiti stabiliti al titolo III, capi 2 e 3, della [legge sull'IA] o una persona soggetta agli obblighi del fornitore a norma [dell'articolo 24 o dell'articolo 28, paragrafo 1, della legge sull'IA], le condizioni di cui al paragrafo 1, lettera a), sono soddisfatte unicamente se l'attore ha dimostrato che il fornitore o, se del caso, la persona soggetta agli obblighi del fornitore non ha rispettato uno dei requisiti stabiliti da tali capi e indicati di seguito, tenendo conto delle misure adottate nel quadro del sistema di gestione dei rischi e dei relativi risultati a norma [dell'articolo 9 e dell'articolo 16, lettera a), della legge sull'IA]:
   (a) il sistema di IA è un sistema che utilizza tecniche che prevedono l'uso di dati per l'addestramento di modelli e che non è stato sviluppato sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui [all'articolo 10, paragrafi da 2 a 4, della legge sull'IA];
   (b) il sistema di IA non è stato progettato e sviluppato in modo da soddisfare gli obblighi di trasparenza di cui [all'articolo 13 della legge sull'IA];
   (c) il sistema di IA non è stato progettato e sviluppato in modo da consentire una supervisione efficace da parte di persone fisiche durante il periodo in cui il sistema di IA è in uso a norma [dell'articolo 14 della legge sull'IA];
   (d) il sistema di IA non è stato progettato e sviluppato in modo da conseguire, alla luce della sua finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza a norma [dell'articolo 15 e dell'articolo 16, lettera a), della legge sull'IA]; oppure
   (e) non sono state immediatamente adottate le azioni correttive necessarie per rendere il sistema di IA conforme ai requisiti stabiliti [dal titolo III, capo 2, della legge sull'IA] o per ritirarlo o richiamarlo, a seconda dei casi, a norma [dell'articolo 16, lettera g), e dell'articolo 21 della legge sull'IA].

3. In caso di domanda di risarcimento del danno presentata contro un utente di un sistema di IA ad alto rischio soggetto ai requisiti stabiliti al titolo III, capi 2 e 3, della [legge sull'IA], la condizione di cui al paragrafo 1, lettera a), è soddisfatta se l'attore dimostra che l'utente:
   (a) non ha rispettato l'obbligo di utilizzare il sistema di IA o di monitorarne il funzionamento conformemente alle istruzioni per l'uso che accompagnano il sistema o, se del caso, l'obbligo di sospenderne o interromperne l'uso a norma [dell'articolo 29 della legge sull'IA]; oppure
   (b) ha esposto il sistema di IA a dati di input sotto il suo controllo che non sono pertinenti alla luce della finalità prevista del sistema a norma [dell'articolo 29, paragrafo 3, della legge sull'IA].

4. In caso di domanda di risarcimento del danno riguardante un sistema di IA ad alto rischio, l'organo giurisdizionale nazionale non applica la presunzione di cui al paragrafo 1 se il convenuto dimostra che l'attore

può ragionevolmente accedere a elementi di prova e competenze sufficienti per dimostrare l'esistenza del nesso di causalità di cui al paragrafo 1.

5. In caso di domanda di risarcimento del danno riguardante un sistema di IA che non è ad alto rischio, la presunzione di cui al paragrafo 1 si applica solo se l'organo giurisdizionale nazionale ritiene eccessivamente difficile per l'attore dimostrare l'esistenza del nesso di causalità di cui al paragrafo 1.

6. In caso di domanda di risarcimento del danno presentata contro un convenuto che ha utilizzato il sistema di IA nel corso di un'attività personale non professionale, la presunzione di cui al paragrafo 1 si applica solo se il convenuto ha interferito materialmente con le condizioni di funzionamento del sistema di IA o se il convenuto aveva l'obbligo ed era in grado di determinare le condizioni di funzionamento del sistema di IA e non l'ha fatto.

7. Il convenuto ha il diritto di confutare la presunzione di cui al paragrafo 1.

2. Il Consiglio d'Europa: Carta etica e raccomandazione

2018

- *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 3-4 dicembre 2018
  La Commissione europea per l'efficacia della giustizia (CEPEJ) del Consiglio d'Europa ha fissato alcuni principi etici relativi all'uso dell'IA nei sistemi giudiziari (tutela dei diritti fondamentali, prevenire possibili discriminazioni, robustezza e sicurezza dei dati, trasparenza, controllo umano). Si afferma l'importanza dell'IA anche nell'ambito della giustizia rilevando l'esigenza di un uso conforme alla Convenzione europea dei diritti dell'uomo (CEDU) e alla Convenzione del Consiglio d'Europa per la protezione dei dati a carattere personale.

2020

- *Raccomandazione del Comitato dei Ministri del Consiglio d'Europa agli Stati membri sugli impatti dei sistemi algoritmici sui diritti umani*, 8 aprile 2020
  Il Consiglio d'Europa ha illustrato il rischio di violazione dei diritti umani da parte di sistemi basati sugli algoritmi individuando delle linee guida elaborate con funzione preventiva. Ad esempio, non dovrebbero essere ammessi i sistemi che comportano un elevato rischio di violazione dei diritti umani.

2022

- Il 7 giugno 2022 il Comitato direttivo sui diritti umani nel campo della biomedicina e della salute (CDBIO) del Consiglio d'Europa ha pubblicato un rapporto sull'impatto dell'IA sulla relazione medico-paziente.
  Questo rapporto, elaborato nel quadro del «Piano d'azione strategico sui diritti umani e le tecnologie nel campo della biomedicina (2020-2025)», esamina i sistemi di IA che interessano la relazione medico-paziente in relazione ai principi dei diritti umani contenuti nella Convenzione europea sui diritti umani e la biomedicina, nota anche come "Convenzione di Oviedo", sottoscritta il 4 aprile 1997 dagli Stati del Consiglio d'Europa.
  In particolare, il rapporto stilato da Brent Mittelstadt esamina il potenziale impatto dell'IA sui diritti umani secondo sei temi: (i) disuguaglianza nell'accesso a cure sanitarie di alta qualità, (ii) trasparenza per gli operatori sanitari e i pazienti, (iii) rischio di pregiudizio sociale nei sistemi di IA, (iv) indebolimento della considerazione del benessere del paziente, (5) rischio di condizionamento dell'automazione, dequalificazione e spostamento della responsabilità e (v) impatto sul diritto alla privacy.

3. L'Italia e il Programma strategico nazionale per l'Intelligenza Artificiale

2018

- *Libro bianco dell'IA al servizio del cittadino*
  Presentato il 21 marzo 2018 dall'Agenzia per l'Italia digitale (AGID) il Libro bianco dell'IA al servizio del

cittadino è il risultato di un lavoro di consultazione e approfondimento che ha coinvolto circa un centinaio di soggetti pubblici e privati. In esso sono illustrate le linee guida e raccomandazioni per l'impiego sostenibile e responsabile dell'IA nella pubblica amministrazione a vantaggio dei cittadini.

2021

- *Programma Strategico nazionale per l'Intelligenza Artificiale (IA) 2022-2024*
  Pubblicato il 24 novembre 2021, il programma è in linea con il piano coordinato dell'Unione europea sull'IA del 7 dicembre 2018. In particolare, esso stabilisce le condizioni per lo sviluppo dell'IA in Italia, concentrandosi sulla cooperazione, sui dati e sull'infrastruttura informatica nonché sulla formazione dei ricercatori e l'importanza degli investimenti nella ricerca, nonché sull'adozione dell'IA e delle sue applicazioni, nella pubblica amministrazione e nei settori produttivi.

4. La giurisprudenza su Intelligenza Artificiale e diritto

4.1. Giustizia amministrativa

2018

- *Algoritmo - procedimento amministrativo*
  «Un algoritmo, quantunque, preimpostato in guisa da tener conto di posizioni personali, di titoli e punteggi, giammai può assicurare la salvaguardia delle guarentigie procedimentali che gli artt. 2, 6, 7, 8, 9, 10 della L. 7 agosto 1990, n. 241 hanno apprestato, tra l'altro in recepimento di un inveterato percorso giurisprudenziale e dottrinario» (T.A.R. Lazio Roma, Sez. III bis, 10 settembre 2018, n. 9224).

2019

- *Algoritmo - procedimento amministrativo*
  «Gli istituti di partecipazione, di trasparenza e di accesso, in sintesi, di relazione del privato con i pubblici poteri non possono essere legittimamente mortificati e compressi soppiantando l'attività umana con quella impersonale, che poi non è attività, ossia prodotto delle azioni dell'uomo, che può essere svolta in applicazione di regole o procedure informatiche o matematiche. A essere inoltre vulnerato non è solo il canone di trasparenza e di partecipazione procedimentale, ma anche l'obbligo di motivazione delle decisioni amministrative, con il risultato di una frustrazione anche delle correlate garanzie processuali che declinano sul versante del diritto di azione e difesa in giudizio di cui all'art. 24 Cost., diritto che risulta compromesso tutte le volte in cui l'assenza della motivazione non permette inizialmente all'interessato e successivamente, su impulso di questi, al Giudice, di percepire l'iter logico-giuridico seguito dall'amministrazione per giungere ad un determinato approdo provvedimentale» (T.A.R. Lazio Roma, Sez. III bis, 27 maggio 2019, n. 6607).
- *Procedimento di formazione della decisione amministrativa*
  «Non vi sono ragioni di principio o concrete, per limitare l'ammissibilità dell'uso di algoritmi informatici nel procedimento di formazione della decisione amministrativa all'attività vincolata della P.A. piuttosto che a quella discrezionale, essendo entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse. In disparte la stessa sostenibilità a monte dell'attualità di una tale distinzione, atteso che ogni attività autoritativa comporta una fase quantomeno di accertamento e di verifica della scelta ai fini attribuiti dalla legge, se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini predetti, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità» (Conferma T.A.R. Lazio n. 6607 del 2019) (Cons. Stato, 4 febbraio 2020, n. 881, *Quotidiano Giuridico*, 2020).
- *Decisione amministrativa automatizzata - condizioni*
  «La decisione amministrativa automatizzata, assunta mediante l'utilizzo di un algoritmo, impone che: a) l'algoritmo sia "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico; b) la regola algoritmica sia non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo» (Riforma T.A.R. Lazio Roma, n. 12026 del 2016) (Cons. Stato, 8 aprile 2019, n. 2270, *Quotidiano Giuridico*, 2019).

- *Decisione amministrativa automatizzata - regola algoritmica*
  «L'utilizzo di procedure "robotizzate" di decisione della P.A., tramite algoritmi, per quanto legittimo, non può essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa. La regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima, anche se ciò avviene in via esclusiva. L'algoritmo, ossia il software, deve essere considerato a tutti gli effetti come un "atto amministrativo informatico". La regola algoritmica: - possiede una piena valenza giuridica e amministrativa, anche se viene declinata in forma matematica, e come tale deve soggiacere ai principi generali dell'attività amministrativa, quali quelli di pubblicità e trasparenza, di ragionevolezza, di proporzionalità, etc.; - non può lasciare spazi applicativi discrezionali (di cui l'elaboratore elettronico è privo), ma deve prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili; la discrezionalità amministrativa è da rintracciarsi al momento dell'elaborazione dello strumento digitale; - vede sempre la necessità che sia l'amministrazione a compiere un ruolo ex ante di mediazione e composizione di interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo (soprattutto nel caso di apprendimento progressivo e di deep learning); - deve contemplare la possibilità che sia il giudice a dover svolgere, per la prima volta sul piano "umano", valutazioni e accertamenti fatti direttamente in via automatica, con la conseguenza che la decisione robotizzata impone al giudice di valutare la correttezza del processo automatizzato in tutte le sue componenti» (Cons. Stato, 8 aprile 2019, n. 2270, *Quotidiano Giuridico*, 2019).
- *Decisione amministrativa automatizzata - trasparenza - conoscibilità dei dati*
  «La decisione amministrativa automatizzata, di per sé legittima, impone al giudice di valutare in primo luogo la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione. Da qui, come si è detto, si conferma la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo. In secondo luogo, il giudice deve poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo, di cui si è ampiamente detto» (Cons. Stato, 8 aprile 2019, n. 2270, *Quotidiano Giuridico*, 2019).
- *Provvedimento amministrativo - algoritmo - trasparenza - conoscibilità*
  «In materia di ricorso ad algoritmi per l'adozione di provvedimenti amministrativi, anche alla luce della disciplina di origine sovranazionale, assumono rilievo fondamentale due aspetti preminenti, quali elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati e l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo. Sul versante della piena conoscibilità, rilievo preminente ha il principio della trasparenza, da intendersi sia per la stessa P.A. titolare del potere per il cui esercizio viene previsto il ricorso allo strumento dell'algoritmo, sia per i soggetti incisi e coinvolti dal potere stesso» (Conferma T.A.R. Lazio Roma, Sez. III, n. 9230/2018.) (Cons. Stato, 13 dicembre 2019, n. 8472, *massima redazionale, Wolters Kluwer*, 2019).

2020

- *Decisione amministrativa - algoritmo - ammissibilità*
  «Ai fini dell'ammissibilità del ricorso ad algoritmi informatici nel procedimento di formazione della decisione amministrativa, assumono rilievo fondamentale, anche alla luce della disciplina di origine sovranazionale, due aspetti preminenti, quali elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati; b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo» (Conferma T.A.R. Lazio n. 6607 del 2019) (Cons. Stato, 4 febbraio 2020, n. 881, *massima redazionale, Wolters Kluwer*, 2020).
- *Provvedimenti amministrativi - algoritmo - trasparenza*
  «In caso di ricorso ad algoritmi per l'adozione di provvedimenti amministrativi, la "caratterizzazione multidisciplinare" dell'algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" ad essa sottesa e che la rendano leggibile e comprensibile. Con le già individuate conseguenze in termini di conoscenza e di sindacabilità. In senso contrario non può assumere rilievo la riservatezza delle imprese produttrici

dei meccanismi informatici utilizzati i quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza» (Cons. Stato, 4 febbraio 2020, n. 881, *massima redazionale, Wolters Kluwer*, 2020).

2021

- *Intelligenza artificiale - algoritmo*
  «Non deve infatti confondersi la nozione di "algoritmo" con quella di "intelligenza artificiale", riconducibile invece allo studio di "agenti intelligenti", vale a dire allo studio di sistemi che percepiscono ciò che li circonda e intraprendono azioni che massimizzano la probabilità di ottenere con successo gli obiettivi prefissati. È possibile allora comprendere che esistono anche algoritmi di intelligenza artificiale, vale a dire algoritmi, tecniche computazionali, soluzioni che siano in grado di replicare il comportamento umano: sono tali, ad esempio, quelli che interagiscono con l'ambiente circostante o con le persone, che apprendono dall'esperienza (machine learning), che elaborano il linguaggio naturale oppure che riconoscono volti e movimenti». (T.A.R. Lombardia Milano, Sez. II, 31 marzo 2021, n. 843).
- *Bando di gara - intelligenza artificiale - algoritmo*
  «Ai fini dell'ottenimento della fornitura di un dispositivo medico con elevato grado di automazione non occorre che l'amministrazione faccia espresso riferimenti a elementi di intelligenza artificiale, essendo del tutto sufficiente, anche in considerazione della peculiarità del prodotto (pacemaker dotati, per definizione, di una funzione continuativa di "sensing" del ritmo cardiaco e di regolazione dello stesso), il riferimento allo specifico concetto di algoritmo, ossia ad istruzioni capaci di fornire un efficiente grado di automazione, ulteriore rispetto a quello di base, sia nell'area della prevenzione che del trattamento delle tachiaritmie atriali» (Cons. Stato, 25 novembre 2021, n. 7891, Sito *Diritto dei Servizi Pubblici.it*, 2022).

4.2. Corte di cassazione

2019

- *Sistemi di intelligenza artificiale - provvedimenti inibitori*
  «L'hosting provider attivo è il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito per la cui prevenzione è ammessa la pronuncia di inibitoria che imponga di bloccare, con le adeguate misure tecniche di "intelligenza artificiale", l'accesso ad un video di contenuto illecito da qualsivoglia indirizzo web (c.d. dynamic injunction)» (Cass. civ., 19 marzo 2019, n. 7708, nota di F. Ferrari, *L'intelligenza artificiale nell'esecuzione di provvedimenti inibitori*, in "Rivista di Diritto Processuale", 2019, n. 4-5, pp. 1343-1354).

2021

- *Sistema automatizzato - algoritmo reputazionale*
  «In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati» (Cass. civ., ordinanza 25 maggio 2021, n. 14381, nota di D. Lafratta, *Algoritmo reputazionale tra requisiti normativi e dignità della persona*, in "Il lavoro nella giurisprudenza", 2022, pp. 154-159.).

5. La dottrina su intelligenza artificiale e diritto

(Relativa ai testi normativi proposti in materia di IA e contenuti nella Risoluzione del PE del 20 ottobre 2020, nella Proposta di Regolamento del Parlamento e del Consiglio pubblicata dalla Commissione europea il 21 aprile 2021 e nella Proposta per una direttiva del Parlamento e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale dell'intelligenza artificiale (Direttiva sulla responsabilità dell'IA), pubblicata dalla Commissione europea il 28 settembre 2022).

5.1. Sulla Risoluzione del Parlamento europeo del 20 ottobre 2020

a) Commenti in generale

G. Taddei Elmi, S. Marchiafava, *Commento*, in G. Taddei Elmi, A. Contaldo (a cura di), "Intelligenza artificiale. Algoritmi giuridici. Ius condendum o fantadiritto", Pacini Giuridica, Pisa, 2020, pp. 281 e ss.

P. Serrao d'Aquino, *La responsabilità civile per l'uso di sistemi di intelligenza nella Risoluzione del Parlamento europeo 20 ottobre 2020: "Raccomandazioni alla Commissione sul regime di responsabilità civile e intelligenza artificiale"*, in "Diritto Pubblico Europeo - Rassegna online", 2021, n. 1, pp. 248-262.

b) Commenti sulla personificazione dei Sistemi di Intelligenza Aritificiale (SIA)

b.1) Favorevoli ad attribuire una futura personalità giuridica ai SIA ai fini di individuare le responsabilità

V. Papakonstantinou, P. de Hert, *Refusing to award legal personality to AI: Why the European Parliament got it wrong*, in European Law Blog/AIRégulation.Com, November, 25th 2020.
Gli autori, partendo proprio dalle considerazioni svolte in sede di Risoluzione del 2020 sul regime di responsabilità civile per l'intelligenza artificiale, muovono ferme critiche al testo, ritenendo che il riconoscimento di una personalità elettronica non diluirebbe il livello di protezione dei consumatori, ma lo aumenterebbe inserendo nuovi soggetti, peraltro più facilmente individuabili da coloro che avrebbero subito dei danni a causa dell'agire autonomico di queste. Nel testo si rilevano, inoltre, i vantaggi che l'istituzione di una personalità elettronica condurrebbe, sintetizzabili (i) nella flessibilità ("flexibility") e (ii) nella sua prossimità ("proximity"). Il primo consente di creare una nuova soggettività di genere terzo, capace di adattarsi al meglio ai vari settori del diritto. Il secondo permette agli utilizzatori di poter agevolmente individuare il soggetto responsabile in quanto il più prossimo alla condotta malevola. Riconoscere il SIA come centro di imputazione di diritti e doveri agevolerebbe, quindi, la parte debole del rapporto nell'immediata individuazione del "responsabile".

S. Wojtczak, *Endowing Artificial Intelligence with legal subjectivity*, in "AI & Society", vol. 37, 2021, pp. 205-213.
Rigetta il mito che il criterio della soggettività giuridica sia la sensienza (percezione-sensazione) e la ragione (intellezione). Argomentando che la IA potrebbe avere una potenziale soggettività giuridica basata in analogia con gli animali o le persone giuridiche ("juristics") suggerisce l'esistenza di una singola gerarchia o sequenza di entità organizzate secondo il loro grado di somiglianza agli esseri umani; inoltre propone che la posizione di una entità in questa gerarchia determina la portata della soggettività attribuita a essa. Il vero criterio della soggettività sarebbe, a parere dell'autrice, la partecipazione e la presenza della IA nella vita sociale, con un qualche ruolo che ancora però oggi non appare significativo.

Una tale soggettività giuridica attribuita sarà ineluttabile, e sempre più cogente, allorquando i SIA acquisiranno uno spazio determinante nella vita sociale. Sul punto l'autrice ricostruisce il filo che legherebbe la soggettività giuridica alla partecipazione nella vita sociale e quindi, il suo connotato, in ultima istanza, di fatto sociale e pre-giuridico. Caratteristiche della presenza sociale sembrano essere la capacità di ricoprire un ruolo all'interno della rete comunitaria, non necessariamente quindi l'attiva partecipazione alla vita della stessa, ed il possesso di un valore connaturato all'esperienza nella vita sociale che possa assumere significato. Una volta che le macchine intelligenti, oggi ancora oggetti, parteciperanno alla vita sociale e saranno ritenute dal sentire comune come socialmente importanti, il passaggio a soggetti di diritto sarà naturale, se non necessaria conseguenza. Questo passaggio da cosalità a soggettività non sarà caratterizzato per il livello quantitativo del lavoro svolto dalla macchina, ma per quello qualitativo, ovvero per il suo mutamento di ruolo. Riconosce che un qualche tipo di soggettività produrrebbe potenziali inevitabili danni che dovrebbero essere presi in considerazione immediatamente e non successivamente.

Tale teoria sembrerebbe, quindi, riprendere e fare proprie le tesi elaborate anche da Teubner, a proposito dei "flussi informativi" come soggetti elettronici: diverrebbero persone solo quando nel processo comunicativo raggiungono un'identità sociale riconoscibile, conquistata, secondo varie gradualità in ragione della capacità di agire di volta in volta riconosciuta.

b.2) Contrari, scettici e "aperturisti" per il futuro sulla personificazione dei SIA

U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in "Rivista di diritto civile", 2020, n. 6, pp. 1247 ss.
Con riguardo alla Risoluzione del 20 ottobre 2020, il modello normativo proposto dal Parlamento europeo, volto a rendere responsabile l'operatore, è in linea con il modello della Commissione europea. Tale modello è basato sul concetto di attività ad alto rischio, definita in relazione alla gravità dei possibili danni, al grado di autonomia della macchina, alla probabilità del danno, e alle modalità o al contesto di utilizzo dello strumento. La distinzione tra attività ad alto rischio e altre attività è centrale ai fini della responsabilità e potrebbe consentire di adottare un regime flessibile per coloro che utilizzano i dispositivi di IA, tra l'altro coerente per alcuni versi al quadro normativo adottato nel 2004 in tema di responsabilità ambientale.

S. Chesterman, *Artificial intelligence and limits of legal personality*, in "International & Comparative Law Quarterly", vol. 69, 2020, n. 4, pp. 819-844.
Analizzando il ruolo dei SIA in relazione al diritto penale, alla responsabilità civile ed alla protezione dell'attività creativa critica le ragioni funzionali che solitamente promuovono il riconoscimento di una soggettività giuridica in capo alle macchine. Ritiene, però, che se, *rebus sic stantibus*, gli ordinamenti prevedono già istituti idonei a regolare l'attività attuale della IA, non si può escludere che in un prossimo futuro possano vedere la luce esseri sintetici dal valore morale comparabile all'uomo ed a quel punto il riconoscimento di uno status comparabile alle persone naturali.

K. Ziemianin, *Civil legal personality of artificial intelligence. Future or utopia?*, in "Internet Policy Review. Journal on internet regulation", vol. 10, 2021, n. 2.
La giurista polacca muovendo dal parallelismo tra ordinamento nazionale e normativa europea nega, per il momento, la necessità di approdare ad una nuova persona elettronica risultando sufficienti le categorie e gli strumenti tradizionali per risolvere i gap normativi causati dalla IA anche con riguardo al riparto della responsabilità civile. La responsabilità per danni prodotti dalla IA deve essere a carico delle persone fisiche, delle persone giuridiche o delle entità con capacità giuridica. I principi di questa responsabilità dovrebbero dipendere dal tipo di IA e dai suoi avanzamenti tecnologici. Il diritto civile deve essere modificato in questo senso e adattato alle esigenze che l'lA pone al diritto. Tali mutamenti dovrebbero essere realizzati gradualmente ma alcuni dovrebbero essere presi in considerazione come *ius condendum*.
Attualmente il risarcimento per i danni subiti causati da IA può essere stabilito solo in base alle regole dei prodotti difettosi. Ritiene però che in futuro la funzione risarcitoria della responsabilità da fatto illecito potrebbe giustificare l'attribuzione ("granting") di una personalità giuridica alla IA. Questo potrebbe comportare la semplificazione delle regole in materia di responsabilità per i sistemi di IA totalmente imprevedibili. Solo questa soluzione potrebbe rendere possibile il risarcimento dei danni ("redress damage") nei confronti della parte danneggiata.

M. Kovac, *Autonomous Artificial Intelligence an Uncontemplated Hazards: Towards Optimal: Regulatory Framework*, in "European Journal of Risk", vol. 13, 2022, n. 1, pp. 94-113.
Dopo la Risoluzione del PE del 2020 aderisce in modo critico contro i fautori della persona elettronica, suggerendo di collocare le questioni di responsabilità della IA nelle categorie giuridiche esistenti senza creare una nuova personalità giuridica elettronica.

5.2. Commenti alla Proposta di regolamento pubblicato dalla Commissione europea (*Artificial Intelligence Act*) il 21 aprile 2021

a) Commenti in generale

F.A. Nanni, *Analisi della Proposta di Regolamento sull'intelligenza artificiale pubblicata dalla Commissione europea il 21 aprile 2021*, in "Cyberlaws.it", 2021.
Pubblicato il 16 giugno 2021 è uno dei primi commenti dove si cerca di mettere in evidenza i molti punti di contatto della Proposta con il GDPR come l'auspicio di sanzioni effettive e dissuasive nei confronti di chi viola le regole sulla protezione dei dati personali.

C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437 (pubblicato il 24 agosto 2021).
Si sottolinea il tentativo della Unione europea di creare un quadro regolatorio che bilanci vantaggi e conseguenze delle applicazioni della IA.

G. Marchianò, *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, in ambientediritto.it, 2021, n. 2, pp. 616-637.
Esame della proposta di Regolamento con particolare riferimento all'IA ad alto rischio. La proposta presenta due aspetti sicuramente positivi: prima di tutto l'aver tentato di dare una cornice giuridica all'IA e, di conseguenza, un'armonizzazione del mercato in merito alle stesse. Non risulta invece soddisfacente nella regolamentazione delle IA e oscura appare la parte delle IA ad alto rischio compreso l'allegato a cui si dovrebbe far riferimento. La proposta di regolamento richiede una revisione anche sulla tecnica utilizzata nella redazione della futura norma.

G. Contissa, F. Galli, F. Godano, Ga. Sartor, *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico-giuridica*, in "i-lex. Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 23 dicembre, 2021, pp. 1-36.
Puntuale analisi della proposta di Regolamento. Il contributo mette in luce l'approccio regolatorio promosso dalla UE sottolineandone le carenze e avanzando raccomandazioni politiche.

Rileva che la proposta di Regolamento costituisce il frutto di un processo condiviso nell'alveo delle istituzioni europee, riunendo i diversi aspetti tecnologici, socio-economici e regolativi sottesi allo sviluppo e alla diffusione dell'IA in Europa; rileva inoltre che ha il merito di elaborare una definizione e una classificazione dei diversi sistemi, fornendo un insieme di requisiti e di incombenze per quei sistemi che mettono a rischio i diritti e i valori europei e stabilendo un'architettura di governance e monitoraggio delle tecnologie.

Ne evidenzia però come punti deboli le incertezze nella definizione e classificazione dei sistemi, la genericità del requisito dei metodi statistici, le ambiguità nelle proibizioni, come il *social scoring* pubblico e nei requisiti dei sistemi ad alto rischio (ad es. la sorveglianza umana) e infine le insufficienze nei meccanismi di controllo (si pensi al cd. controllo interno).

Si osserva che a tutti questi aspetti sottendono due elementi di carattere generale rivelatori di una prospettiva complessiva del legislatore europeo, da un lato volta alla protezione dei diritti e delle libertà fondamentali, ma dall'altro largamente influenzata dal modello di legislazione industriale orientata al mercato.

Il primo elemento è costituito dall'approccio top-down della proposta. Il Legislatore identifica le tecnologie dell'AI, predetermina le pratiche proibite e rischiose e identifica ex ante il livello di rischio, facendone derivare le regole applicabili. Parrebbe più adeguato, per la regolazione di tali tecnologie, un approccio bottom-up, basato sull'identificazione delle caratteristiche della tecnologia e dei processi nei quali essa viene utilizzata, specie se si opera in un contesto basato sul rischio. Il metodo top-down comporta il pericolo di creare categorie normative astratte che non rappresentano in modo adeguato caratteri e rischi effettivi delle singole soluzioni tecnologiche.

Il secondo elemento è rappresentato dal fatto che l'impianto complessivo della proposta rivela una contraddizione di fondo fra il piano pubblicistico e quello dei diritti individuali. Le norme intenderebbero regolare il rischio che l'IA crea per i valori e i diritti umani tutelati dall'Unione. La Proposta è però incentrata su obblighi e prerogative del fornitore, dell'utente e del supervisore definendo requisiti di sviluppo dei sistemi, le modalità di utilizzo e certificazione, i meccanismi di controllo. Mentre dei soggetti su cui ricadono le conseguenze dell'utilizzo del sistema non v'è quasi traccia: a chi subisce l'operato del sistema (ad esempio chi si ritrova sorvegliato, indagato, accusato da un'IA) non si conferiscono diritti né strumenti di azione. Il Regolamento, pur proclamando di volere difendere i valori europei e i diritti fondamentali dai rischi dell'IA, non prevede, per perseguire questo obiettivo, nessuno strumento specifico di difesa per i titolari dei diritti coinvolti. Ad esempio il diritto ad ottenere una spiegazione da parte del sistema AI? O il diritto a non essere soggetti a decisioni discriminatorie? L'attenzione all'impatto dell'IA sulle persone, del resto, sarebbe forse stata agevolata da un approccio bottom-up. Partendo ad esempio dalla Carta dei diritti fondamentali dell'Unione europea e stabilendo per ciascun diritto i parametri di misura del rischio legato alla sua violazione (tenendo conto del "peso" di ogni diritto, e del grado di rischio). Sulla base di questi parametri, si sarebbe potuto determinare, di volta in volta, il livello di rischio dello specifico sistema di IA (evitando così il "cherry-picking"), nonché

le misure di protezione individuali. Sarebbe stato così possibile fornire una sorta di diritti "accessori" che rendessero "azionabili" i diritti umani messi in pericolo.

Si rileva infine che la proposta, nel tentativo di coniugare i diritti individuali con le esigenze di mercato relative all'IA, non riesce a trovare un bilanciamento soddisfacente e soluzioni applicative adeguate. Si auspica che il prosieguo del percorso legislativo conduca ad un maggiore equilibrio.

G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale?* in V. Cuocci, F.P. Lops, C. Motti (a cura di), "La responsabilità civile nell'era digitale" (Atti della Summer School 2021), Cacucci, pp. 3-28.
Commenta sia il testo contenuto nella Risoluzione del 20 ottobre 2020 sia il testo contenuto nella Proposta di Regolamento del 2021 e rileva che in entrambe «si avverte, nonostante l'attenzione prestata alla creazione del rischio e alle graduazioni del rischio, l'impossibilità delle istituzioni europee di superare la distinzione tra progettazione dei sistemi di IA e fabbricazione di prodotti che incorporano quei sistemi, poiché l'unificazione dei criteri di imputazione nel segno della responsabilità oggettiva è prevista solo in caso di alto rischio». Per cui si sottolinea «che occorrerà effettuare un attento coordinamento tra le regole di responsabilità da prodotto con le regole di responsabilità dell'operatore per assicurare un adeguato risarcimento delle vittime», p. 21.

G. Finocchiaro, *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, pp. 303-322.
Si sottolinea che il regolamento europeo sarebbe il primo modello organico della materia ma si evidenziano come limiti la rigidità delle definizioni dei SIA (top down), con la conseguente difficoltà di tenere conto degli sviluppi tecnologici, la scarsa distinzione tra i tipi di entità che usano la IA e la difficile compatibilità dell'approccio basato sulla gestione del rischio con un contesto di cooperazione internazionale, che potrebbe portare a un isolamento dell'Europa.

G. Resta, *Cosa c'è di europeo nella Proposta di Regolamento UE sulla intelligenza artificiale*, in "Il diritto dell'informazione e dell'informatica", 2022, n. 2, pp. 323-342.
Facendo ricorso a una tassonomia usuale nell'ambito degli studi di comparative *law and regulation*, la proposta europea delinea 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. Il cardine della proposta sembra 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. In questo senso anche L. Floridi, *The European Legislation on AI: Brief Analysis of its Philosophical Approach*, in "Philosophy & Technology", vol. 34, 2021, pp. 215-222 e D. Bomhard, M. Merkle, *Regulation of Artificial Intelligence. The EU Commission's Proposal of an AI Act*, in "EuCML", 2021, pp. 257 e ss.

b) Commenti sulla Responsabilità civile

G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti"?*, in "Rivista di diritto civile", 2021, n. 1, pp. 823 e ss.
L'autore ritiene che la proposta di introdurre la personalità (o soggettività) elettronica (o digitale) sarebbe condivisibile a condizione che questa personificazione non sia considerata come uno status di «persona» ma solo «quale presupposto del successivo riconoscimento della corrispondente (mera) responsabilità patrimoniale»; quanto al modello dell'emanando *Artificial Intelligence Act* nota una correlazione tra le differenti tipologie di sistemi di IA, segnatamente a rischio elevato e le corrispondenti modalità di immissione nel circuito di utilizzo, con l'individuazione dei soggetti coinvolti «(sia pure con ruoli differenti) rispetto agli obblighi gravanti su ciascuno, con l'obiettivo di garantire adeguati standard di tutela e, soprattutto, assicurare la predeterminazione dei diversi livelli di responsabilità».

A. D'Alessio, *La responsabilità civile dell'intelligenza artificiale antropocentrica*, in "Persona e Mercato", 2022, n. 2, pp. 244-257.
Sulle questioni di responsabilità civile aderisce alle scelte proposte nei testi del 20 ottobre 2022 e del 21 aprile 2021 del PE e della Commissione ritenendo inutile e rischiosa l'attribuzione di una personalità giuridica ai SIA e approvando la «collocazione della responsabilità in capo a una categoria soggettiva in ragione della necessità di evitare secche a cui si giungerebbe dando adesione della personalità giuridica dell'automa e all'ipotesi di nofault insurance» (p. 255).

V. Di Gregorio, *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie*, in "Danno e responsabilità", 2022, n. 1, pp. 51-63.
L'introduzione del regime binario (responsabilità oggettiva per i SIA ad alto rischio e presunzione di colpa in casi definiti e previa una adeguata valutazione per i SIA a basso rischio) determinerebbe la coesistenza di regole in tema di responsabilità diversificate in funzione del livello del rischio del sistema o del prodotto lasciando in vigore con eventuali modifiche le disposizioni sulla responsabilità da prodotto quando questo non rientri nella suddetta categoria tecnologica (pp. 56).

E. Rajneri, *The projects of European regulation on liability for damage caused by artificial intelligence. Striking a balance between the interests of consumers, multinationals and SMEs*, in "Rivista di diritto bancario", 2022, n. 2, pp. 95-119.
Al fine di regolare la responsabilità civile per i danni causati dalla IA non ritiene necessario superare o rimpiazzare la Direttiva sulla responsabilità per i prodotti del 1985. Questa soluzione aumenterebbe la frammentazione normativa che le Istituzione europee intendono limitare. Sarebbe preferibile anche in adesione al conclamato principio della neutralità tecnologica rivedere la Direttiva che era stata progettata in età pre-digitale per renderla applicabile a ogni tipo di prodotto inclusa la IA.

A. Bertolini, *Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies*, in "Europa e diritto privato", 2022, n. 2, pp. 369-420.
Il contributo contesta l'approccio di regolamentazione generale delle applicazioni della Intelligenza artificiale che emerge dalla Risoluzione PE del 20 ottobre 2020 oggi ripresa dalla Proposta di Regolamento del 21 aprile 2021. Si critica l'approccio tecnologico neutrale in riferimento alla responsabilità civile suggerita.

Affronta la nozione di "sistema di intelligenza artificiale" (SIA) e il suo effetto sulla certezza del diritto, la distinzione, artificiale e insufficiente, tra applicazioni ad alto e basso rischio e i corrispondenti diversi regimi di responsabilità proposti. Cerca di dimostrare, attraverso esempi (es.: negligenza medica) come ciò potrebbe incidere profondamente sugli incentivi all'adozione anticipata di applicazioni più avanzate, accrescendo l'onere a carico dei convenuti, che potrebbe includere il medico stesso.

Discute la nozione di "operatori" per mostrare come ciò comporterà l'aumento del numero di potenziali responsabili, causando rilevanti incertezze rispetto al contenzioso secondario e alle azioni di regresso e limitazioni al danno risarcibile.

Ribadisce infine che la responsabilità civile nelle tecnologie avanzate dovrebbe occuparsi principalmente del risarcimento dei danneggiati e non della sicurezza del prodotto. Quest'ultima dovrebbe essere affrontata attraverso la regolamentazione sulla sicurezza dei prodotti.

F. Astone, *Artificial intelligence: ipotesi per una regolazione normativa*, in V. Cuocci, F.P. Lops, C. Motti (a cura di), "La responsabilità civile nell'era digitale" (Atti della Summer School 2021), Cacucci, pp. 30-44.
Dopo una analisi generale della proposta, dove si sottolinea il taglio minimalista suggerito dalla Commissione europea in relazione «a una responsabilità semi-oggettiva (si prevede una prova liberatoria che richiede la prova della forza maggiore) accompagnata dalla scelta di imporre una assicurazione obbligatoria», critica il definitivo abbandono della ipotesi di una personificazione del SIA giudicando deboli gli argomenti contrari (pp. 41-44).

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

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0083

Recensione a: Barbara Giovanna Bello, Laura Scudieri (a cura di), *L'odio online: forme, prevenzione e contrasto*, Torino, Giappichelli, 2022

Casimiro Coniglione

Il volume curato da Barbara Giovanna Bello e Laura Scudieri, ottava pubblicazione della collana "Diritto e vulnerabilità – Studi e ricerche del CRID" diretta da Thomas Casadei e Gianfrancesco Zanetti, analizza le manifestazioni dell'odio online attraverso un approccio interdisciplinare.

L'odio, com'è noto, è un sentimento di forte e persistente avversione, in cui si desidera il male o la rovina del prossimo. La fruizione della rete può essere associata al Giano bifronte: da un lato, permette di interagire con utenti e piattaforme di tutto il mondo, arricchendo così la propria esperienza socioculturale; dall'altro lato, ha amplificato il discorso d'odio nei confronti dei gruppi più vulnerabili, sia per l'utilizzo dell'anonimato, sia per la durata – tendenzialmente – indeterminata dei contenuti d'odio nel Web. Siffatti contenuti, tra l'altro, corrono il rischio di un "ritorno imprevedibile", poiché possono essere conservati dagli utenti e riproposti dopo un certo lasso di tempo.

L'obiettivo delle curatrici e degli autori/autrici è quello di indagare il discorso d'odio online fornendo interessanti spunti di riflessione sulla sua manifestazione, il contrasto e la prevenzione del fenomeno.

Il contributo di Bello e Scudieri – dopo aver analizzato il "significato" dell'odio, inteso come strumento di negazione dell'altro e proiezione di timori personali, riversati nei confronti della vittima – si sofferma sulle difficoltà degli Stati a fronteggiare il fenomeno. Su questa materia, su cui risulta difficile trovare un accordo, la *soft law* pare prevalere sull'*hard law*. Come opportunamente analizzato dalle autrici, questa difficoltà si scontra all'interno di due concezioni di base sulla libertà di manifestazione del pensiero: la prima, di origine statunitense (e assai favorevole alle grandi piattaforme del Web), si basa sul concetto del *marketplace of ideas* (locuzione adottata dal *Justice* Oliver Wendell Holmes) e propugna l'assenza di un censore che limiti la manifestazione delle idee; la seconda, di matrice europea, invece, giustifica la limitazione alla manifestazione del pensiero nei casi in cui si perpetui una violazione alla dignità dell'uomo e nei casi di discriminazione.

Nonostante le difficoltà e le diverse lacune del diritto a regolamentare un fenomeno di quest'ampia portata, è interessante notare che tre Stati membri dell'Unione europea (Germania, Austria e Francia) hanno adottato una legislazione per il contrasto del discorso d'odio online (sulle buone pratiche legislative, si veda anche il contributo di B.G. Bello, *I discorsi d'odio in rete*, in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer-Cedam giuridica, 2021, pp. 257-260).

La riflessione di Stefania Cavagnoli è incentrata sull'immenso potere della lingua per dispensare odio. Partendo dagli studi di pragmatica linguistica di John Searle e John Langshaw Austin, che sostenevano la potenza dell'atto linguistico come azione in grado di modificare la realtà, l'autrice sofferma la propria analisi sull'uso dell'epiteto, che – provenendo in

C. Coniglione è dottorando di ricerca in Lavoro, Sviluppo, Innovazione, Università degli Studi di Modena e Reggio Emilia – Fondazione Marco Biagi.

genere da un registro linguistico più basso – è in grado di possedere una considerevole forza discriminante nei confronti di chi lo subisce. La lingua, inoltre, è in grado di incentivare un discorso d'odio anche nei casi in cui omette (volontariamente) di pronunciare il genere grammaticale femminile – molto opportunamente l'autrice fa notare che l'omissione della pronuncia di una parola nel suo corrispettivo femminile (si pensi, ad esempio, ad avvocata, sindaca o assessora) è una forma di discorso d'odio, seppur meno violento rispetto al classico discorso d'odio, perché non riconosce il ruolo della donna, pretende e incentiva la lingua come costrutto prettamente maschile, che privilegia solo – ed esclusivamente – il genere maschile.

Cavagnoli, poi, concentra la propria riflessione sullo strumento dell'immagine. Anche l'immagine è un veicolo per il discorso d'odio: non rispettare i canoni estetici dell'odierna società, e condivisi dalla cultura di riferimento, significa essere vittima – ad esempio – di *bodyshaming* attraverso l'uso di un linguaggio violento.

L'analisi di Scudieri indaga invece il concetto di ironia nel discorso d'odio. L'ironia (dal greco εἰρωνεία, ovvero dissimulazione) è un particolare strumento del discorso d'odio che, in via indiretta, esprime il contrario di ciò che si afferma. Nell'epoca dei social network non è raro imbattersi in *meme* (immagini ad alto contenuto ironico) che ridicolizzano le competenze femminili, legittimando uno stile narrativo-argomentativo a vantaggio delle competenze maschili e assai discriminatorio nei confronti delle donne: la peculiarità dei *meme* sta nel fatto che nella rete il messaggio ironico-discriminatorio è recepito da un indeterminato numero di utenti e *communities*. Inoltre, l'ironia gioca un ruolo cruciale anche all'interno della fattispecie incriminatrice del *revenge porn*.

L'autrice – sulla scia della riflessione giusfilosofica di Catherine MacKinnon – sottolinea come l'ironia a favore di uno stupro legittima e consolida un set di credenze patriarcali e stereotipate che considerano la donna come un mero strumento per la consumazione di un rapporto sessuale. E se è vero che l'ironia esprime il contrario di ciò che afferma, è altrettanto vero che il comportamento sessuale consumato ai danni della donna scaturisce – seguendo il ragionamento stereotipato dell'uomo – da una "supposta" devianza femminile (si pensi, ad esempio, al noto caso di Tiziana Cantone). A questo proposito, Scudieri auspica – sin dalla scuola dell'infanzia – una "didattica dell'ironia" per sensibilizzare le nuove generazioni sull'uso distorto dell'ironia.

La riflessione di Matteo Botto evidenzia la significativa presenza dei *The red pillars*: un gruppo nato su Reddit (un sito Internet nato nel 2005 che ha come scopo la pubblicazione di social news, intrattenimento e forum in cui intrattenere discussioni su diversi argomenti) che rivendica l'egemonia del potere maschile a discapito di quello femminile. L'ideologia di questo gruppo è quella di sottolineare la superiorità del potere maschile rispetto a quello femminile; a sostegno delle loro argomentazioni, presentano argomenti biologici quali, ad esempio, la superiorità del corpo e la capacità dell'uomo a svolgere più mansioni contemporaneamente. I *redpillers*, protagonisti indiscussi del discorso d'odio di genere, incolpano sia le femministe sia gli attivisti colpevoli, a loro avviso, della "crisi della mascolinità". Particolarmente interessante, poi, è che questo gruppo possa essere considerato espressione di *prosumers*, ossia utenti che producono contenuti online (in modo particolare attraverso la creazione di *meme*) e fruiscono dei suddetti contenuti.

Miguel Angel López-Saéz, Lucas R. Platero e Andrea Angulo Menassé analizzano il discorso d'odio online nei confronti delle persone LGTBQI+ in Spagna. In modo particolare, nel contributo viene evidenziato che le vittime del discorso d'odio online, a causa del loro orientamento sessuale, soffrono di un notevole livello di stress dettato dalla loro identità; questo stress può indurre le vittime a tenere propositi autolesionistici. L'uso della rete da parte di questo gruppo vulnerabile ha effetti sia positivi che negativi: gli effetti positivi sono legati all'opportunità di interazione con persone trovando conforto e confronto; gli effetti negativi, invece, sono legati alla sovraesposizione, e, di conseguenza, ai discorsi d'odio. In modo particolare, durante la pandemia da COVID-19 in Spagna e il conseguente *lockdown*, i ragazzi e le ragazze LGTBQI+ hanno sofferto un notevole aumento di stress perché innanzi a loro si profilavano due scelte: fare il *coming out* in famiglia oppure continuare l'esperienza online, al costo di nascondere la propria identità sessuale nel mondo offline. Questo contributo mostra assai bene la necessità di implementare una pedagogia dell'ascolto (anche tramite forum professionali in rete), in modo tale da ridurre il livello di stress e fornire una risposta seria ai bisogni dei giovani LGTBQI+ che tenga conto delle loro necessità e della loro vulnerabilità.

L'indagine di Giovanni Ziccardi e Pierluigi Perri – condotta attraverso gli strumenti d'analisi dell'informatica giuridica – evidenzia come i contenuti d'odio online si siano immedesimati all'interno dei big data, sfruttando proprio le caratteristiche dei big data: l'amplificazione dei messaggi; la persistenza dei contenuti, ossia la difficolta di cancellazione dei contenuti una volta inseriti all'interno della rete;

la viralità, cioè la grande capacità dei contenuti a circolare in maniera incontrollata all'interno della rete. Ad avviso degli autori, la generazione dei contenuti d'odio (anche grazie alla grande mole di dati inseriti all'interno del Web – ceduti per usufruire di servizi a titolo gratuito) presenta diverse caratteristiche: la potenza; la precisione e la segretezza. Una risposta a questo fenomeno, sempre ad avviso degli autori, può provenire dal GDPR (Regolamento generale per la protezione dei dati personali) integrando l'art. 2 del GDPR con il Considerando 18 e attraverso la figura del *content provider*.

In modo particolare – seguendo il ragionamento della sentenza della Corte europea per i diritti dell'uomo, *Delfi As v. Estonia* – il provider ha un'ampia capacità di controllo dei contenuti rispetto all'utente. Anche il nostro ordinamento, infatti, ha esteso questa capacità di controllo al Garante per la protezione dei dati personali, riconoscendo un potere di blocco verso i provider qualora le informazioni siano classificabili come cyberbullismo.

Anche se questa attività di monitoraggio e controllo del Garante è dedicata alla fattispecie del cyberbullismo, non è escluso che per analogia possa essere applicata al discorso d'odio online.

Il contributo di Sara De Vido indaga la lacuna legislativa del discorso d'odio online basato sul genere; anche in questo caso, sono presenti atti di *soft law* (che, ad ogni buon conto si ricorda, non sono vincolanti). La pandemia, tra l'altro, ha esasperato il discorso d'odio di genere e le conseguenze di siffatto comportamento è la normalizzazione di queste pratiche nei confronti delle donne e la riduzione delle stesse all'auto-censura, fuorviate da una narrativa distorta che mira a favorire un'inesatta auto-rappresentazione dell'identità femminile. Un decisivo riconoscimento legislativo del discorso d'odio di genere potrebbe avvenire, ad avviso dell'autrice, attraverso l'inserimento dello stesso come euro-crimine. Infatti, una modifica dell'art. 83 del Trattato sul funzionamento dell'Unione europea, e l'elevazione del discorso d'odio di genere a reato, potrebbe essere un primo riconoscimento a tutela dei gruppi sociali più vulnerabili.

Ciò nonostante, come opportunamente fa notare l'autrice, la criminalizzazione del comportamento senza un adeguato piano di protezione (come, ad esempio, la rimozione del contenuto lesivo) e senza un adeguato piano di prevenzione, renderebbe vana la sensibilizzazione su siffatte questioni.

La riflessione di Giacomo Viggiani indaga gli aspetti sostanziali e processuali della legge 29 maggio 2017, n. 71, che rappresenta per il nostro ordinamento la prima – e finora unica – definizione sul cyberbullismo. La legge, inoltre, a tutela della vittima, ha previsto l'istanza di oscuramento, rimozione o blocco del contenuto e la procedura di ammonimento; quest'ultimo procedimento ha una natura amministrativa e svolge, sostanzialmente, una funzione dissuasiva a livello psicologico sull'autore del reato: da una parte, si fa affidamento sull'autorevolezza del questore per ammonire il cyberbullo e tentare una conciliazione con la vittima; dall'altra parte, si vuole insistere sull'auto-responsabilizzazione del cyberbullo. È particolarmente interessante la presenza di aspetti educativi e organizzativi all'interno della legge, che intende affidare al Ministero dell'istruzione il compito di redigere delle Linee di orientamento per la lotta al cyberbullismo e l'obbligo per le istituzioni scolastiche di nominare un referente per il cyberbullismo, con il preciso compito di istituire piani di prevenzione e di contrasto del fenomeno.

Nonostante gli innegabili intenti positivi della normativa, la mancanza di fondi rende del tutto inapplicabile la funzione pedagogica-culturale.

Annalisa Verza, nel suo contributo, analizza la funzione dello *story-telling*, ossia della narrazione come strumento che modella le credenze condivise di una società; nel mondo online le narrazioni del discorso d'odio online mirano a "recuperare" il privilegio del potere maschile perso a causa dell'affermazione del giusfemminismo. Le narrazioni di questi gruppi tendono a rappresentarsi come "vittime" del c.d. "sesso debole" e accusano la società moderna di aver portato uno squilibrio nei rapporti uomo-donna.

Un'attenzione particolare viene mostrata nei confronti della "Generazione Z", ossia quella generazione di ragazzi e ragazze nati/e tra il 1995 e il 2010 che è cresciuta insieme alle nuove tecnologie. La loro identità è completamente plasmata dai social network: la velocità e la brevità dei messaggi online ha ridotto anche la capacità critica di elaborazione e assimilazione dei contenuti. Da ciò si evince sia una maggiore reattività di questi utenti ai messaggi, sia una maggiore emotività nel recepire i messaggi. Ad avviso dell'autrice, l'educazione civica (con lo studio delle regole della convivenza da parte di studenti e studentesse) e la didattica del diritto dovrebbero educare i ragazzi e le ragazze della generazione Z, fornendo una solida capacità critica di elaborazione dei contenuti e una valida difesa verso le narrative d'odio in cui potrebbero essere vittime.

È necessario, ad avviso di Verza, costruire narrazioni alternative, in pieno equilibrio con i valori democratici ed egualitari, a discapito di quelle attuali che invece favoriscono una narrazione unilaterale e antidemocratica.

L'ultimo contributo del volume, ossia quello di Bello, intende analizzare le forme di attivismo digitale. L'autrice – dopo aver descritto attraverso le esperienze degli autori della *Critical Race Theory* i disagi patiti dalla vittima del discorso d'odio razzista, ovvero l'auto-rappresentazione di sé stessi come esseri inferiori rispetto al "gruppo dominante" – evidenzia anche le grandi opportunità offerte con l'attivismo digitale. Bello, a questo proposito, distingue tre forme di attivismo digitale: la prima tipologia di attivismo è l'*affermazione di sé*, promosso dal singolo e dai gruppi sociali bersagliati dal discorso d'odio per poter affermare e difendere la propria identità innanzi all'aggressore; la seconda tipologia di attivismo è quella della società civile, ossia da parte del singolo, gruppi o operatori giuridici (soggetti terzi rispetto alla vittima) che si prodigano a difesa del singolo o del gruppo sociale colpito dal discorso d'odio; la terza – e ultima – tipologia di attivismo è quello promosso dalle istituzioni in sinergia con le fasce della popolazione più giovane. L'autrice, a questo proposito, fa luce su una campagna promossa dalle istituzioni per fronteggiare il discorso d'odio come il *No Hate speech movement* – che propone un coinvolgimento di ONG giovanili, forum, istituzioni pubbliche nazionali e internazionali. In Italia, i referenti del *No Hate speech movement* sono il Dipartimento della Gioventù e il Servizio Civile Nazionale. La partecipazione dei giovani è incentivata attraverso l'*e-partecipation*, ossia attraverso la partecipazione online dei giovani. L'auspicio dell'autrice è quello che queste tipologie di attivismo digitale, forniscano un antidoto al veleno del discorso d'odio: la rete può essere un utile strumento per rispondere a un odio immotivato e per riaffermare la propria identità innanzi all'aggressore, o gli aggressori, della rete.

Nel complesso, il volume mostra assai bene le diverse manifestazioni dell'odio online, che è assai persistente e duraturo, potendo raggiungere un numero indeterminato di utenti e restare (sempre a tempo indeterminato) all'interno del Web, colpendo la persona o gruppi già vulnerabili, contribuendo così ad acuire le discriminazioni nei loro confronti e a generare erronee auto-rappresentazioni della propria identità, a causa di una "supposta" superiorità dell'aggressore.

Come puntualmente osservato da Federico Faloppa nella *Postfazione* del volume, per poter comprendere, lottare e sconfiggere il discorso d'odio online serve «un continuo sforzo di approfondimento, in grado di sfidare rigidità definitorie, rendite di posizionamento, luoghi comuni e semplificazioni o eccessivamente consolatorie o istericamente allarmistiche».