RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da Sebastiano Faro e Marina Pietrangelo

In questo numero

Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati

SEZIONE MONOGRAFICA

a cura di
S. Calzolaio

1 2021

Anno III, n. 1/2021 • 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

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto
Periodico internazionale del CNR-IGSG
Anno III • n. 1/2021 • Periodicità semestrale
www.rivistaitalianadiinformaticaediritto.it

Direzione
Sebastiano Faro e Marina Pietrangelo

Comitato di direzione
Federigo Bambi, Davide Carnevali, Gian Luca Conti, Rosa Maria Di Giorgi, Elio Fameli
Enrico Francesconi Erik Longo, Elisabetta Marinai, Stefano Pietropaoli, Francesco Romano
Giancarlo Taddei Elmi

Comitato scientifico nazionale
Laura Abba, Agata C. Amato Mangiameli, Andrea Cardone, Antonio Carcaterra, Paolo Caretti
Massimo Carli, Enrico Carloni, Adriana Ciancio, Renato Clarizia, Giuseppe Corasaniti
Pasquale Costanzo, Giovanna De Minico, Carla Faralli, Giusella Finocchiaro, Tommaso E. Frosini
Mario Jori, Donato A. Limone, Aldo Loiodice, Luigi Lombardi Vallauri, Nicola Lupo
Nicoletta Maraschio, Paolo Moro, Monica Palmirani, Ugo Pagallo, Giovanni Pascuzzi
Dianora Poletti, Oreste Pollicino, Giovanni Sartor, Andrea Simoncini, Carlo Sorrentino
Lara Trucco, Stefano Trumpy, Alessandra Valastro, Franco Vallocchia, Giovanni Ziccardi

Comitato scientifico dei corrispondenti stranieri
Y. Amoroso (C), T.J.M. Bench Capon (GB), D. Bourcier (F), W. 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, Enrico Albanesi, Maria Romana Allegri, Marco Bassini, Raffaella Brighi
Elda Brogi, Simone Calzolaio, Giuseppe Cammarota, Gianluigi Ciacci, Sofia Ciuffoletti
Maria Vittoria Dell'Anna, Fabio Dell'Aversana, Rossana Ducato, Paolo Galdieri, Riccardo Gualdo
Paolo Guarda, Antonio Iannuzzi, Alessandro Lovari, Daniele Marongiu, Paola Marsocci
Letizia Materassi, Erica Palmerini, Saulle Panizza, Anna Papa, Paolo Passaglia, Viviana Patti
Giovanni Piccirilli, Benedetto Ponti, Cecilia Robustelli, Andrea Rossetti, Simone Scagliarini
Caterina Sganga, Giuseppe Vaciago, Giulia Venturi

Redazione tecnica
Simona Binazzi (segreteria), Giuseppina Sabato (composizione dei testi), Elisabetta Marinai (sito web)

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

Direttore responsabile
Sebastiano Faro

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

Indice

Sezione monografica

***Ubi data, ibi imperium*:**
IL DIRITTO PUBBLICO ALLA PROVA DELLA LOCALIZZAZIONE DEI DATI
a cura di Simone Calzolaio

5 **Simone Calzolaio**
Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati

11 **Valentina Pagnanelli**
Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali

27 **Vanni Boncinelli**
Modelli tecnici e disciplina giuridica del c.d. cloud computing

47 **Stefano Torregiani**
La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa

67 **Yuan Li**
Cross-border Data Transfer Regulation in China

Studi e Ricerche

79 **Ciro D'Urso**
I profili informatici nella valutazione della responsabilità dell'Hosting Provider

89 **Alessandra Vernice**
Il letto di Procuste dei sistemi informativi via Web: un pluralismo falsato?

103 **Elena Montagnani**
La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia: quali prospettive future?

139 **Laura Abba**
Carenze attuali e soluzioni future nei meccanismi per la cooperazione digitale

149 **Kelvin Peroli, Cíntia Rosa Pereira de Lima**
Democrazia come *Value-Sensitive Design*: un approccio sociotecnico allo sviluppo delle tecnologie basate su principi democratici

157 **Enrico Albanesi**
Roberto Zaccaria, Alessandra Valastro, Enrico Albanesi, *Diritto dell'informazione e della comunicazione*, XI edizione, Milano, Wolters Kluwer-Cedam, 2021

163 **Alessio Facciorusso**
Gianluigi Fioriglio, *Informatica medica e diritto. Un'introduzione*, Modena, Mucchi Editore, 2020

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0035

Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati

Simone Calzolaio

La sezione della *Rivista italiana di informatica e diritto* ospita una serie di contributi in merito al regime giuridico della conservazione e della circolazione dei dati nella società digitale. Si intende introdurre sul piano metodologico il problema giuridico della localizzazione e disponibilità dei dati, come profilo attinente alla sovranità dello Stato contemporaneo.

Localizzazione dei dati – Sovranità digitale – Disponibilità dei dati – Dipendenza dai dati – Datificazione

Sommario: *1. Datificazione, Intelligenza artificiale,* data dependence – *2.* Ubi data, ibi imperium*: descrivere e individuare le questioni aperte, sotto il profilo giuridico – 3. Localizzazione dei dati, cognizione delle informazioni. Profili soggettivi della disponibilità di dati e informazioni – 4. Segue: profili oggettivi. La localizzazione e i suoi molteplici volti. L'ordinamento costituzionale al tempo della* data dependence.

1. Datificazione, intelligenza artificiale, *data dependence*

La realtà attuale rappresenta un contesto *data intensive*. Nel corso degli ultimi anni, ad avviso di chi scrive[1], la nozione che si presta meglio a descrivere la situazione attuale, anche per consentire una comprensione complessiva del fenomeno della cd. realtà digitale o altrimenti noto come *big data*, è quella di datificazione (*datification* o *datafication*).

La *datification* si compone di tre fattori essenziali: l'aumento esponenziale della quantità di dati prodotti nel mondo; la capacità di analisi dei dati e di estrazione di informazioni dai dati, svolta da parte di macchine a ciò addestrate; la possibilità e la capacità di prendere decisioni attraverso queste nuove informazioni, anche grazie alla cd. *alghoritmic decision making*.

Negli ultimi anni, la *datification* ha rappresentato un terreno fertile per lo sviluppo di tecnologie basate sull'intelligenza artificiale.

Le tecniche di *machine learning*, *deep learning*, *data mining* hanno bisogno di enormi quantità di dati, di buona qualità, per perfezionarsi, per riuscire a fornire a trarre informazioni dai dati e, di conseguenza, servizi sempre più raffinati e specifici.

L'insieme di questi fattori evidenzia che siamo in un contesto di *data driven innovation*; l'innovazione si realizza attraverso lo sfruttamento dei dati. In tutti i settori, e trasversalmente.

Ciò significa che anche la competizione e la concorrenza fra aziende, stati, continenti si gioca nella progressione della capacità di sfruttamento dei dati.

Questi aspetti lasciano capire perché il possesso e la disponibilità dei dati sono strategici, per le imprese, per gli stati, e per le imprese che operano nei diversi Stati.

Di più. Questo momento storico caratterizzato dalla pandemia rende evidente che l'avvento della *datification* e la *data-driven innovation* conducono ormai ad un contesto di data *dependence*[2]: non si tratta di sviluppare complessi ragionamenti, ma di

S. Calzolaio è professore associato di Diritto costituzionale presso il Dipartimento di Scienze politiche, della comunicazione e delle relazioni internazionali dell'Università degli Studi di Macerata.

arrendersi al fatto che il corso, il fluire, lo sviluppo della vita personale, sociale, economica, istituzionale dipende dal e segue il flusso dei dati. Siamo dipendenti dalla garanzia della continuità del flusso dei dati e delle informazioni per comunicare, esprimerci, operare, lavorare, vivere.

2. *Ubi data, ibi imperium*: descrivere e individuare le questioni aperte, sotto il profilo giuridico

Allo stato attuale, quindi, il contesto tecnologico, ma si potrebbe ben dire la realtà dei fatti, richiede al giurista uno sforzo non indifferente, che lambisce la domanda in ordine alla sua stessa identità e alle esigenze cognitive necessarie a consentire una comprensione dell'esistente e poi una regolazione giuridica orientata ai principi del costituzionalismo liberaldemocratico[3].

In qualche modo, in particolare sul versante del diritto pubblico, si sta sviluppando un vero e proprio diritto dei dati, che trae molte delle sue caratteristiche e dei suoi connotati dal modello europeo della protezione dei dati personali, ma che non coincide più e non si riduce più né alla protezione dei dati personali, né al diritto della proprietà intellettuale.

Il diritto pubblico è quella branca del diritto che si occupa – nel costituzionalismo occidentale – di regolare, e quindi di limitare, il potere dello Stato e di garantire la sovranità dello Stato e la tutela dei diritti delle persone (cittadini e non cittadini).

Il contesto tecnologico attuale, l'avvento della rete internet, del mondo digitale, della *datification* e dell'intelligenza artificiale, introduce un collegamento strutturale, e non temporaneo, fra disponibilità dei dati da parte degli Stati e *imperium*, cioè capacità di esercizio del potere sovrano. Con espressione sintetica: *ubi data, ibi imperium*.

L'espressione tuttavia va subito puntualizzata, senza pretesa alcuna di esaustività, sotto due profili.

Bisogna subito sottolineare che, in questo caso, perfino il termine "ubi" può e deve essere letto e declinato secondo le categorie del nuovo contesto tecnologico. Il luogo individuato dall'*ubi* può non essere uno spazio fisico, un territorio statale, un luogo unico e unitario. Affinché sia soddisfatta la formula (*ubi*... *ibi*...), non è affatto necessario pensare l'*ubi* come un luogo localizzato nel territorio dello Stato (su questo si veda il contributo di Valentina Pagnanelli).

Anche perché – ed ecco la seconda osservazione preliminare – affinché possa essere esercitato l'*imperium*, cioè il potere sui dati, quel che conta non è tanto la localizzazione dei dati, ma quella delle informazioni che se ne traggono e si riesce a trarne immediatamente e/o per correlazione con altri dati e altre informazioni (su entrambi questi aspetti – nei termini che di seguito si tenta di delineare – appare decisamente utile il contributo di Vanni Boncinelli).

Per queste ragioni, per il fatto di dover tener conto di un contesto tecnologico in cui il concetto di territorio si viene rimodulando, così come alcuni aspetti concernenti la distinzione fra popolo e popolazione, ed il correlativo concetto di monopolio del potere e della forza, si ritiene che il diritto pubblico sia chiamato ad una prova importante, forse epocale, come in realtà quasi tutti i settori della ricerca scientifica di fronte a questa quarta rivoluzione (secondo la lettura di Luciano Floridi[4]).

Quale metodo seguire per affrontare l'indagine scientifica della rivoluzione digitale in corso, anche solo rispetto al tema evocato, che tuttavia, come si intuirà, non è affatto facile anche solo da perimetrare?

Si ritiene, sommessamente, che il metodo debba necessariamente, in questa fase, essere descrittivo e interrogativo. Non ancora, o almeno non immediatamente, prescrittivo. Vi è infatti molto più da descrivere, da domandare e da capire, per il giurista (e non solo), di quanto si sia in grado di prescrivere con certezza o di certificare attraverso una prescrizione. Il primo passo di questa prova, pertanto, consiste nell'aprirsi non solo a nuovi temi, ma alle nuove categorie implicate dalla rivoluzione digitale: descrivere la fenomenologia, i nuovi istituti e concetti che emergono dall'esperienza, classificarli con timore e tremore, per avviarsi a comporre il nuovo mosaico del diritto pubblico dell'era digitale.

Qui non si sostiene affatto che mutino principi, diritti, criteri tipici e tradizionali del diritto pubblico. Non lo si può escludere apriori, ma è infantile trarre una conclusione del genere prima di descrivere analiticamente le fattispecie rilevanti e la loro intrinseca connessione. D'altra parte – come pure ancora il contributo di Vanni Boncinelli appare prospettare e fondare – non è affatto detto che un approccio tradizionale (localizzando i dati in un certo territorio statale si può garantire l'accesso illimitato alle informazioni portate da quei dati) sia in grado di raggiungere gli obiettivi prefissati (infatti, fra dato e informazione può collocarsi una capacità di criptografia dei dati che rende impossibile, allo Stato, l'accesso alle informazioni, pur essendo tutti i dati localizzati all'interno del territorio sovrano dello Stato). Pertanto, appunto, la questione prioritaria per il giurista è, in questo momento, riuscire a descrivere fattispecie che presentano un grado di novità

consistente. E questo è il tentativo che si sviluppa negli articoli di questa sezione.

3. Localizzazione dei dati, cognizione delle informazioni. Profili soggettivi della disponibilità di dati e informazioni

Di chi sono i dati? La domanda può apparire banale. In riferimento ai nostri dati personali tutti risponderemmo "i dati sono senz'altro miei!". Ovviamente non abbiamo letto le policies dei social network che utilizziamo!

Infatti, la domanda non è affatto banale. E la risposta non è affatto chiara o univoca.

I dati che circolano e sono prodotti in Italia, di chi sono? Cioè, a chi appartengono e chi può avervi accesso? Chi può analizzarli e di chi sono le informazioni che se ne ricavano?

Qui evidentemente non si possono affrontare e tantomeno risolvere questi quesiti.

Si può però osservare che un aspetto consistente dell'indagine scientifica dovrebbe necessariamente riguardare il rilievo pubblico e/o privato dei dati, e la relativa regolazione, pubblica e privata. In Cina – è sufficiente leggere l'articolo seguente di Yuan Li – hanno iniziato a porsi il problema, e con esiti interessanti sul piano del modello di disciplina (si pensi alla nozione di *important data* ed al relativo regime, che supera la ormai incompleta bipartizione europea dati personali/non personali).

In altri termini, è arrivato il momento che il diritto pubblico (altra questione in campo: il diritto pubblico italiano o europeo?) inizi a definire con una certa precisione quale è la situazione giuridica soggettiva che caratterizza il rapporto fra soggetto (privato e pubblico) e dato, e fra soggetto e informazione.

Cosa significa esattamente essere titolari dei dati? Cosa significa avere la disponibilità dei dati? Cosa significa aver diritto di accesso ai dati? Chi ha il diritto di utilizzare i dati? Questi diritti sono esclusivi? Il titolare dei dati è il proprietario? È il possessore? È il detentore? È una nuova figura giuridica che esula dagli istituti tradizionali del diritto "continentale" (*trust/trustee*)? E in che relazione è lo Stato con i dati e le informazioni, il cui insieme si rivela decisivo per garantire sicurezza, progresso, sovranità interna ed esterna dello Stato stesso?

Come è noto, almeno sotto il profilo del diritto della protezione dei dati personali, il GDPR offre una serie di risposte a questi quesiti. Ma si tratta ancora di risposte iniziali, parziali, nel senso che si riferiscono appunto ai dati personali, cioè a qualsiasi informazione concernente una persona fisica identificata o identificabile.

Il regolamento Europeo del 2018, concernente la libera circolazione dei dati non personali, non offre al momento risposte soddisfacenti o esaustive a queste domande (e su questo si veda il contributo di Stefano Torregiani).

Evidentemente, l'Unione europea si sta muovendo per edificare, progressivamente, un regime giuridico europeo dei dati, che si costruisce attraverso l'allargamento delle direttive esistenti in materia di comunicazioni elettroniche e di sistemi audiovisivi alle problematiche poste dai sistemi di messaggistica istantanea (Whatsapp) e dalle piattaforme audiovisive online (Netflix)[5].

Ma ancora più importante sarà il *digital service act*, cioè un vero e proprio diritto delle piattaforme online, e l'insieme di regolamenti, direttive e azioni che l'Unione europea – si badi quindi, non uno Stato, ma un ordinamento *sui generis* – sta mettendo in campo[6].

Tuttavia, quel che qui interessa è sottolineare – sulla scia di un recente convegno scientifico internazionale – quale sia il regime giuridico del *what people leave behind*, e quindi la descrizione progressiva di quale sia la relazione soggettiva fra persona, impresa, istituzioni e dato/informazione.

4. Segue: profili oggettivi. La localizzazione e i suoi molteplici volti. L'ordinamento costituzionale al tempo della *data dependence*

In questo contesto, ha ormai preso forma un problema più specifico, di cui si avviano ad occuparsi sotto profili diversi tutti i contributi che seguono.

Interi ordinamenti hanno iniziato a comprendere la rilevanza strategica della raccolta dei dati sul territorio nazionale ed i rischi implicati dal travolgente avvento del fenomeno del *cloud computing*.

Per questo, hanno iniziato a introdurre disposizioni volte a vincolare al territorio la raccolta e conservazione dei dati o a ostacolare il flusso verso l'esterno dei dati.

Il diritto dei dati, pertanto, ha iniziato a porre limiti ed a porsi in contrapposizioni ai caratteri genetici della rete internet, che consentono l'ubiquità dei dati e potenzialmente lo sfruttamento dei dati in modo simultaneo e intensivo.

Si sono affacciati nel contesto del dibattito scientifico i temi della localizzazione dei dati, della sovranità sui dati e della sovranità digitale dello Stato, il tema del regime del *trans-border data flow*, il

rischio del *data colonialism*, o all'inverso del *digital isolationism*, e infine la nuova tendenza al *data nationalism*.

Come ha puntualmente osservato Chander: «we define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms-including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data»[7].

Secondo la sua tesi, la localizzazione dei dati finisce per compromettere, invece che garantire, la sicurezza e la privacy di dati/informazioni e agevola il potere di sorveglianza degli Stati.

L'aspetto più interessante, per chi scrive, di questo contributo non consiste tanto nelle conclusioni cui perviene (che ciascuno verificherà se sono o meno condivisibili), ma specificamente nell'osservazione tecnologica del contesto in cui la localizzazione dei dati si colloca. Infatti, ad es., egli ritiene che vi sia un importante problema di sicurezza dei dati nel fatto che singoli Stati si occupino, con i loro limitati mezzi, della sicurezza di data set, in luogo dei grandi operatori del settore che, per definizione, hanno standard di sicurezza più elevati e aggiornati.

È una osservazione importante. Infatti, molti notano l'attivismo dell'Unione europea sul fronte della disciplina giuridica, sotto molteplici profili, dei dati, delle piattaforme, del commercio elettronico, ecc., e il connesso rischio di ipertrofia normativa.

Ma in pochi hanno notato l'iniziativa congiunta francese e tedesca per la costituzione di GAIA X, cioè di una "federated data infrastructure for Europe"[8].

Come viene esposto proprio nella presentazione del progetto – ormai già avviato – l'Europa sviluppa importanti investimenti in tecnologie digitali a modelli innovativi di business. Per questo: «we must ensure that those who drive innovations forward are also those who benefit in economic terms. This will help to secure value creation and employment in Europe. An open digital ecosystem is needed to enable European companies and business models to compete globally. This ecosystem should allow both the digital sovereignty of cloud services users and the scalability of European cloud providers. Within GAIA-X, we are developing the foundations for a federated, open data infrastructure based on European values. GAIA-X connects centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. The resulting federated form of data infrastructure strengthens the ability to both access and share data securely and confidently».

In altri termini, attraverso l'iniziativa francese e tedesca, l'Europa si sta dotando di una infrastruttura *cloud* tutta europea, dedicata a ospitare dati (importanti?) europei.

La questione della collocazione sicura, tecnologicamente all'avanguardia e conforme a standard di protezione dei dati personali (e non), appare tutt'altro che un problema o un tema astratto.

Ovviamente anche in Italia, con i tempi e i modi italiani, si sta ponendo il problema: il d.l. 21 settembre 2019, n. 105, convertito con modificazioni dalla l. 18 novembre 2019, n. 133, disciplina e determina, con ampi margini di approssimazione, il perimetro di sicurezza nazionale cibernetica[9].

Quel che qui interessa sottolineare, è che i temi indicati sono aspetti concreti del diritto dei dati che, non sempre in modo organico, sta nascendo e crescendo in Italia e in Europa.

Per poter giocare un ruolo in questo scenario, occorre partire da una prima, provvisoria, parziale descrizione degli aspetti che ne sono alla base, fra tecnologia e diritto.

Il problema della titolarità e della localizzazione dei dati, che è tutto da scrivere e da descrivere, si colloca sullo sfondo di due domande aperte. E in qualche modo contribuisce ad acuirle.

Quale regime di diritto pubblico di titolarità dei dati e di localizzazione dei dati è compatibile con (o ottimale in) una società liberal-democratica? Quale diritto costituzionale dei dati, nel progredire della *data dependence* della società contemporanea?

Ovviamente queste sono le domande del diritto costituzionale dell'era digitale e questo è il modo con cui anche per il diritto pubblico si inizia a porre il problema della cd. realtà aumentata.

Note

[1]Per questa impostazione e per più ampi riferimenti, sia consentito rinviare a S. Calzolaio, voce *Protezione dei dati personali*, in "Dig.disc.pubbl.", 2017, p. 594 ss.

[2]R.D. Taylor, *"Data localization": The internet in the balance*, in "Telecommunications Policy", vol. n. 44, 2020, n. 8.

[3]L. Lessig, *Code 2.0*, Basic Books, 2006.

[4]L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

[5]Interessantissimo, a questo riguardo, il recente aggiornamento del manuale E. Albanesi, R. Zaccaria, A. Valastro, *Diritto dell'informazione e della comunicazione*, Wolters Kluwer-Cedam, XI ed., 2021.

[6]Cfr. Commissione europea, *Strategia europea in materia di dati*.

[7]A. Chander, P.L. Uyen, *Data Nationalism*, in "Emory Law Journal", vol. n. 64, 2015, p. 677-740.

[8]Cfr. *GAIA-X: A Federated Data Infrastructure for Europe*.

[9]Cfr. B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in "Giornale di diritto amministrativo", 2020, n. 5, p. 629 ss.

Introduction. *Ubi data, ibi imperium*: public law facing data localization

Abstract: *The Rivista italiana di informatica e diritto* hosts a series of contributions on the legal regime of data storage and circulation in the digital society. The aim of this contribution is to introduce, on a methodological level, the legal problem of data localization and availability, as a profile pertaining to the sovereignty of the contemporary state.

Keywords: Data localization – Digital sovereignty – Data availability – Data dependance – Datification

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0022

Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali

Valentina Pagnanelli

Utilizzando le politiche di conservazione dei dati nel settore pubblico come paradigma, il contributo offre una riflessione sulle modalità con cui gli Stati stanno affermando o difendendo la loro sovranità digitale. L'articolo propone una ricostruzione del percorso di digitalizzazione della PA italiana, sul quale i *big data* hanno avuto un notevole impatto. La conservazione dei dati digitali ha imposto il passaggio dagli archivi cartacei ai *cloud*, un passaggio regolato dalla normativa nazionale ed europea ed in parte influenzato dalle strategie digitali delle grandi potenze mondiali. Il proliferare di obblighi e divieti di localizzazione conferma la complessità e la centralità di questi temi nella difesa della sovranità digitale. Il contributo si chiude con una analisi dei punti salienti della *European strategy for data* pubblicata dalla Commissione europea nel febbraio 2020, e con uno sguardo al progetto franco-tedesco di conservazione e condivisione dei dati denominato GAIA-X.

Conservazione dei dati – Sovranità digitale – Settore pubblico – Localizzazione dei dati

Sommario: *1. Introduzione – 2. Dalla digitalizzazione ai big data: il nuovo campo da gioco del settore pubblico – 3. La babele dei dati: fine delle classificazioni? – 4. Regole e ruoli per la conservazione dei dati nella PA – 5. L'individuazione delle infrastrutture: dall'archivio digitale al principio del cloud first – 6. Le regole di localizzazione: data storage pubblico e sovranità – 7. Riflessioni conclusive: la strategia digitale europea*

1. Introduzione

The Guardian il 24 aprile 2020 titolava *UK government told not to use Zoom because of China fears*[1]. Nell'articolo si dava conto della circostanza che «Government and parliament were told by the intelligence agencies last week not to use the videoconferencing service Zoom for confidential business, due to fears it could be vulnerable to Chinese surveillance».

Il *National Cyber Security Centre* avrebbe infatti sconsigliato ai membri del Governo e del Parlamento del Regno Unito l'utilizzo della piattaforma di videoconferenze Zoom[2], quantomeno per le riunioni classificate come "riservate"[3].

Il 29 ottobre 2019 durante l'annuale *Digital summit* tedesco[4] è stato presentato il progetto GAIA-X, una infrastruttura cloud interamente europea, interoperabile ed indipendente dai servizi forniti dai providers statunitensi e cinesi. La cancelliera Angela Merkel in quella occasione ha sottolineato l'importanza di trovare soluzioni europee per garantire la sovranità sui dati. Il progetto franco-tedesco[5] propone di implementare un sistema alternativo ai servizi offerti dai giganti del cloud, che assicuri il rispetto di elevati standard etici e di sicurezza e che sia basato sul principio della *data sovereignty by design*, al fine di creare uno spazio comune europeo per la conservazione dei dati[6].

V. Pagnanelli è dottoranda in Scienze giuridiche presso l'Università di Firenze, avvocato, consulente della protezione dati. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

Il 7 aprile 2020, in sede di prime osservazioni sulla app di tracciamento dei contatti per il contenimento del Covid-19 all'esame del gruppo di lavoro istituito dal Governo c.d. *data-driven*[7], il Garante privacy italiano ha richiamato l'attenzione sulla necessità di una scelta oculata dei partner tecnologici, in ragione dell'elevato rischio connesso ai trattamenti di dati personali dei cittadini. Il Garante ha inoltre consigliato di privilegiare soggetti "situati in territorio italiano[8]". In una intervista rilasciata a *Cybersecurity trends* il 16 aprile 2020, il Presidente dell'Autorità garante è tornato sul tema, invocando la evidente necessità di un ripensamento della governance pubblica, per garantire la sovranità digitale dello Stato di fronte alle crescenti minacce globali all'indipendenza dei Paesi: *In uno spazio "defisicizzato" come la rete la sovranità va declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica [...]*[9]".

Territorio, sovranità e potere sono concetti assolutamente attuali nel diritto di internet, con cui bisogna fare i conti[10]. Eloquentemente Oreste Pollicino introduce così un commento a due sentenze della Corte di Giustizia dell'Unione europea[11] nelle quali i giudici di Lussemburgo sono stati chiamati a decidere sulla fissazione dei limiti territoriali all'applicazione del diritto europeo, giungendo peraltro a soluzioni apparentemente contrapposte[12].

Già questa breve e parziale rassegna evidenzia come le categorie costituzionali poc'anzi citate, pur necessitando di essere ripensate, rimangano necessarie per governare il contesto globale digitalizzato dei nostri giorni.

Utilizzando le politiche di conservazione e accesso ai dati del settore pubblico come paradigma, il presente contributo intende offrire una riflessione sulle modalità con cui gli Stati stanno affermando la loro sovranità digitale in una fase storica in cui, da una parte, il territorio diventa un riferimento sfuggente per individuare e proteggere i confini di una giurisdizione che è sempre meno materiale, e dall'altra, i sistemi democratici e le libertà e i diritti dei cittadini sono minacciati dal crescente e pervasivo ricorso all'intelligenza artificiale[13].

2. Dalla digitalizzazione ai big data: il nuovo campo da gioco del settore pubblico

Non ripercorreremo in questa sede le tappe dello sviluppo tecnologico che in alcuni anni, con progressione geometrica, ci ha portato dal cartaceo, al digitale, allo scenario attuale in cui i Big Data e in particolare la Big Data Analytics hanno cambiato di fatto la relazione dell'uomo con le informazioni[14].

Una componente di cruciale importanza all'interno di questa evoluzione è certamente costituita dalla progressiva digitalizzazione del patrimonio informativo delle pubbliche amministrazioni, che le ha portate a disporre di banche dati costantemente alimentate[15], contenenti quantità straordinarie di informazioni, siano esse dati personali, categorie particolari di dati, o dati non personali[16]. La Pubblica Amministrazione italiana, sulla quale la prima parte della trattazione sarà incentrata, non è naturalmente rimasta estranea a questo cambio di paradigma.

Invero a seguito del deciso impulso alla digitalizzazione impresso alle amministrazioni pubbliche in particolare con il d.l. n. 179/2012, che ha portato alla progressiva creazione tra gli altri dell'Anagrafe nazionale delle popolazione residente, del fascicolo elettronico dello studente, del fascicolo sanitario elettronico (istituito dalla Regioni e province autonome), la Pubblica Amministrazione italiana ha assunto *la responsabilità di gestire, trattare, condividere, elaborare, "archivi digitali" immensi, da cui possono essere tratte informazioni in grado di compromettere tanto gli interessi nazionali quanto i diritti individuali*[17].

Il progressivo sviluppo delle *Smart cities* ha contribuito ad incrementare esponenzialmente anche la quantità di dati non personali conservati dalla PA. Tale scenario ha di recente subito una ulteriore spinta in avanti con il Piano Triennale per l'Informatica 2019-2021, elaborato dall'Agenzia per l'Italia Digitale (AgID)[18].

L'introduzione del concetto di *Smart Landscape*[19] segna un importante cambiamento di quello che per lungo tempo è stato l'immaginario collettivo, che collegava la *smartness* ad un ventaglio certamente ampio di servizi e benefits per il cittadino, relegando le imprese e l'industria ai margini dei progetti di volta in volta ideati. Il modello di *Smart Landscape* prevede invece uno sviluppo dei servizi resi alle imprese, prime fra tutte quelle legate alla logistica per la circolazione delle merci.

Vale la pena di segnalare che il Piano Triennale prevede la progressiva implementazione di un modello predittivo (*Smart Landscape Engine*) che dovrà essere impiegato nella governance dello *Smart Landscape*. SLE sarà capace di elaborare scenari *what-if* in base alle informazioni inserite, e dovrà coadiuvare i processi decisionali legati allo sviluppo del *paesaggio intelligente*. La rilevanza di quanto appena descritto appare evidente: la realizzazione di un modello di intelligenza artificiale della PA segna infatti

un ulteriore avvicinamento[20] del settore pubblico a tecnologie (e pratiche) già ampiamente utilizzate nel settore privato.

Trasparenza amministrativa e *Open data* non costituiscono l'oggetto di questo contributo[21]. Basti solo qui ricordare che la governance dei dati del settore pubblico non può, in concreto, prescindere dal considerare anche gli obblighi di pubblicazione, oltre che le garanzie di accessibilità totale e riutilizzo delle informazioni[22]. Tali informazioni, a seguito di una costante ed ineliminabile opera di valutazione e bilanciamento rispetto al diritto alla protezione dei dati personali dei soggetti i cui dati sono di volta in volta coinvolti, contribuiscono in modo significativo ad accrescere l'insieme dei dati che possono essere correlati con altri dati e che rappresentano un fattore di *disclosure globale*[23] di informazioni, personali e non.

La digitalizzazione, lo sviluppo delle ICTs, il progredire dell'Intelligenza Artificiale hanno delle potenzialità eccezionali per il miglioramento della qualità dei servizi nel settore pubblico, oltre che in termini di semplificazione, riduzione dei costi, conoscibilità dell'azione amministrativa, esercizio dei diritti di cittadinanza, corretto svolgimento della vita democratica. I recenti accadimenti globali ne hanno dimostrato l'utilità anche per la gestione di situazioni complesse quali il contenimento di una epidemia (la possibilità di disporre di dati organizzati, unita all'interoperabilità di banche dati afferenti a differenti organismi, pubblici e privati, pare in alcuni casi aver fatto la differenza[24]).

Ma l'accentramento di una quantità incalcolabile di informazioni in una banca dati, unito alla possibilità di incrociare tali informazioni con quelle provenienti da altri database utilizzando algoritmi raffinatissimi, porta con sé altrettanti gravi rischi per i diritti e le libertà dei singoli, soprattutto rispetto a possibili discriminazioni, e per la tenuta dei sistemi democratici, ove le informazioni venissero utilizzate per interferire con la libera formazione dell'opinione pubblica[25] o con lo svolgimento dell'attività politica-economica-amministrativa di uno Stato sovrano[26].

A questo proposito si evidenzia come Garante per la protezione dei dati personali, AGCOM e AGCM, al termine di una analisi conoscitiva congiunta sul fenomeno dei Big Data[27], abbiano espresso preoccupazione in merito alla compatibilità con la normativa in materia di protezione dati di alcuni aspetti delle attività di analisi dei Big Data quali l'indeterminatezza delle finalità, i rischi legati alla possibilità di reidentificazione degli interessati, l'opacità delle logiche applicate dagli algoritmi.

Il report fa un esplicito riferimento alla creazione della Piattaforma Digitale Nazionale Dati, introdotta con l'art. 50 ter del Codice dell'Amministrazione Digitale (CAD). Le criticità della piattaforma andrebbero individuate principalmente nell'accentramento presso un unico soggetto di informazioni *anche sensibili e sensibilissime*, per finalità del tutto generiche, con evidente rischio di usi distorti. Secondo le tre Autorità indipendenti, date queste premesse, un trattamento fondato sui Big Data nel settore pubblico richiederà una base legale idonea *che assicuri ai cittadini, oltre alla trasparenza delle decisioni, la proporzionalità del ricorso ex lege a tale metodologia rispetto all'obiettivo di interesse pubblico perseguito e l'individuazione, nel rispetto del principio di privacy by design, di adeguate garanzie da integrare nel trattamento, dopo aver accuratamente valutato i rischi elevati per i diritti e le libertà degli interessati*[28].

3. La babele dei dati: fine delle classificazioni?

L'espansione del fenomeno della Big data Analytics sembra aver messo in luce i limiti del processo, divenuto ormai macchinoso, di separazione dei dati in categorie. Infatti molto spesso tale attività, seppure realizzabile in una fase di ricognizione ex ante dei dataset, diviene di poca utilità ex post, ovvero a seguito del trattamento degli stessi dati con strumenti di machine learning: com'è noto, infatti, grazie a raffinatissimi algoritmi, oggi possiamo estrarre informazioni personali su un individuo anche a partire da informazioni che personali non sono[29].

L'utilizzo di algoritmi applicati ad un volume immenso di dati consente di estrarre o anche di prevedere informazioni personali, a volte partendo da dataset di informazioni non personali, correlati con altri dataset di differente origine e contenuto[30]. In questo contesto la distinzione tra dato personale e dato non personale dunque è sempre meno realizzabile[31], e la possibilità di una applicazione di regimi giuridici differenti a tipologie diverse di dati, sempre meno probabile.

Una differenziazione che, qualora effettivamente possibile, comporterebbe comunque un aumento di spesa per adeguamenti tecnologici e probabili impegni regolamentari interni alle Pubbliche amministrazioni, che appaiono di difficile realizzazione nel breve periodo. Anche nel settore privato, un onere siffatto comporterebbe un sensibile aumento di costi e una riduzione del valore dei dati medesimi.

Il problema si pone oggi in concreto a seguito della entrata in vigore del Regolamento europeo c.d. FFD (*Free Flow Data*) sulla circolazione dei dati non personali, che introduce un regime differenziato per tutti i dati che non rientrino nella definizione[32] (e

nella disciplina) contenuta nel GDPR. Com'è noto, la possibile difficoltà nella separazione tra i due insiemi di dati è stata già prevista dal legislatore europeo, che all'art. 2 par. 2 del Regolamento n. 1807/2018 precisa che qualora i dati personali e non personali all'interno di un dataset siano indissolubilmente legati, resta impregiudicata l'applicazione del GDPR. A parere di chi scrive, tale inquadramento normativo costituirà un impedimento non di poco conto alla libera circolazione di una grandissima mole di dati non personali, inscindibilmente legati, tuttavia, a dati personali[33].

Proseguendo nella rassegna delle tipologie di dati, con specifico riferimento ai trattamenti posti in essere dalle amministrazioni pubbliche, vi è un ulteriore criterio di classificazione che nella prassi si rivela molto impattante. Si tratta della distinzione tra insiemi di dati contenuti in documenti cartacei e dataset che costituiscono i documenti digitali della PA. La citata distinzione non è meramente formale, ma come si vedrà tra un attimo è al contrario collegata ad aspetti assolutamente sostanziali.

Ancora una volta è il Regolamento FFD a fare da spartiacque, infatti in esso il *trattamento* viene definito come *qualsiasi operazione o insieme di operazioni compiute su dati o insiemi di dati in formato elettronico*[34]. Come poc'anzi ricordato, il Regolamento FFD pone regole volte ad agevolare la libera circolazione dei dati, che sono applicabili, appunto, solamente ai trattamenti di dati in formato elettronico.

I dati non personali contenuti in documenti cartacei, sono dunque de facto esclusi dalla disciplina che ne regola la libera circolazione nel territorio dell'Unione europea. Non considerare l'esistenza di questo "doppio binario" rischia di restituire una visione parziale della realtà; questa peculiarità invece potrebbe provocare limitazioni non secondarie alla applicazione della normativa, riducendone in ultima analisi l'efficacia.

4. Regole e ruoli per la conservazione dei dati nella PA

I riferimenti normativi generali in materia di conservazione degli atti della Pubblica Amministrazione e di gestione degli archivi sono contenuti nel D.P.R. n. 445/2000, in particolare nell'art. 68[35]. La medesima disposizione pone l'obbligo di applicazione della normativa in materia di privacy a tutte le attività di gestione e custodia dei documenti. Sarà dunque qui utile richiamare rapidamente le regole di *data storage* poste dal GDPR.

Il Regolamento UE n. 2016/679 impone al titolare del trattamento[36] di conservare i dati personali per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati, con due sole eccezioni: che i soggetti cui i dati personali si riferiscono non siano più identificabili; che i dati siano trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici (art. 5 par. 1 lett. e).

Il GDPR impone inoltre al titolare del trattamento di informare l'interessato rispetto al periodo di conservazione dei dati personali, o perlomeno di indicare i criteri utilizzati per determinare tale periodo (art. 13 par. 2 lett. a). Come si vedrà a breve, anche il responsabile del trattamento[37] deve cancellare o restituire i dati personali al titolare una volta terminata la prestazione (art. 28 par. 3 lett. g). Nel Registro dei trattamenti vanno indicati, quando possibile, i termini ultimi di cancellazione per ciascuna categoria di dati personali (art. 30 par. 1 lett. f).

A parere di chi scrive vi sono due aspetti della disciplina privacy sulla conservazione che incidono significativamente, e più di altri, nella governance dei dati del settore pubblico.

Il primo di essi è dato dalla applicazione dell'art. 25 del Regolamento 2016/679. La norma impone al titolare del trattamento di mettere in atto misure tecniche e organizzative atte a garantire la protezione dei dati e a tutelare in questo modo i diritti degli interessati. Tali misure dovranno essere individuate a seguito di una valutazione effettuata caso per caso, per ogni differente fattispecie di trattamento, *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche [...]*.

La conseguenza diretta della applicazione del principio di privacy by design appena descritto a quello che nel paragrafo precedente abbiamo chiamato "doppio binario" è evidente: l'attività di conservazione dei documenti amministrativi sarà soggetta ab origine a due differenti discipline, a seconda che i documenti siano cartacei o digitali[38].

La presenza di un doppio sistema di conservazione dei dati costituisce peraltro una componente non eliminabile nel breve periodo. Lo conferma la norma del CAD che prevede la predisposizione da parte delle PA di piani di sostituzione degli archivi cartacei con quelli informatici all'esito di una valutazione costi/benefici[39].

Un secondo aspetto, ancor più rilevante, della applicazione della disciplina privacy alla conservazione dei dati nel settore pubblico, è quello che attiene

alla individuazione e nomina dei citati responsabili esterni del trattamento, a norma dell'art. 28 del GDPR.

Il GDPR pone delle regole piuttosto precise per l'attribuzione della responsabilità rispetto al legittimo trattamento dei dati. Al titolare del trattamento spettano le decisioni in merito alle finalità e ai mezzi del trattamento. I responsabili sono invece soggetti che trattano i dati per conto del titolare e sono a tal fine "incaricati" con contratto o altro atto giuridico vincolante. Tale atto contiene la regolamentazione del rapporto tra titolare e responsabile[40], le istruzioni impartite dal primo e gli obblighi per il secondo rispetto al trattamento dei dati personali.

Nel contesto della Pubblica Amministrazione molte attività sono gestite da soggetti esterni incaricati a seguito di bando o tramite affidamento diretto. Ciò significa che in moltissimi settori, quantità consistenti di dati siano trattate esternamente.

In questa sede non è possibile neppure accennare al complesso organigramma dei "ruoli privacy" risultante dalla rete di rapporti che legano la PA ad altri soggetti pubblici e ad imprese e professionisti del settore privato. Sia consentito, tuttavia, rilevare come il rispetto della normativa sulla protezione dati abbia imposto alcuni adempimenti anche durante la pandemia di Covid-19. Il rispetto del GDPR e del Codice privacy ha infatti imposto alle autorità statali di elaborare rapidamente disposizioni normative che hanno consentito ai numerosi soggetti coinvolti nella gestione dell'emergenza di trattare legittimamente dati personali. Tale attività, seppure incontestabilmente necessaria, ed urgente, ha dato vita ad una rete complessa di ruoli e responsabilità che appare onestamente difficile da ricostruire a posteriori[41].

Terminata la digressione, è necessario a questo punto individuare i soggetti incaricati della conservazione dei dati nella Pubblica Amministrazione, che qualora esterni all'amministrazione medesima, dovranno essere contrattualizzati ex art. 28 del GDPR.

È l'articolo 34 del CAD ad offrire alle pubbliche amministrazioni l'alternativa tra la conservazione dei documenti informatici all'interno della propria struttura organizzativa e l'affidamento di tale attività a soggetti pubblici e privati accreditati presso AgID come conservatori. L'art. 44 impone poi al responsabile della conservazione che decida per l'esternalizzazione, di individuare soggetti che offrano *idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.* Il rispetto di questo ultimo requisito dovrà essere garantito attraverso la predisposizione e sottoscrizione di contratti ex art. 28, che contengano la regolamentazione giuridica del rapporto tra *data controller* e *data processor*, oltre che istruzioni stringenti sulla sicurezza informatica dei dati trattati. La centralità e rilevanza di questo "adempimento privacy" sono state confermate di recente dall'Autorità garante.

Nel parere sullo schema di Linee guida sulla formazione, gestione e conservazione dei documenti informatici[42], reso il 13 febbraio scorso[43],il Garante per la protezione dati personali ha ribadito la necessità per le PA di rispondere ai requisiti richiesti dal GDPR, precisando che una chiara attribuzione dei compiti è il presupposto per una corretta attribuzione delle responsabilità, e che tale suddivisione deve essere contrattualizzata ed esplicitata in clausole che rispondano ai requisiti del Regolamento europeo, a maggior ragione nei casi in cui si preveda di esternalizzare servizi.

Merita evidenziare come il Garante non ponga dei limiti all'affidamento a privati di servizi che prevedano il trattamento di dati personali, ma insista piuttosto nella piena applicazione di tutte le garanzie individuate dal GDPR (contrattualizzazione dei responsabili esterni, rispetto degli obblighi di sicurezza, applicazione dei principi di privacy by design e by default, efficienti procedure di notifica in caso di data breach, adesione a codici di condotta).

Richiamate regole e ruoli del data storage pubblico, ci occuperemo ora del regime relativo alla collocazione materiale dei dati e documenti conservati. Nei prossimi paragrafi si darà conto di almeno due aspetti di rilievo: l'individuazione della tipologia di infrastrutture per l'archiviazione, e le regole di localizzazione dei dati.

5. L'individuazione delle infrastrutture: dall'archivio cartaceo al principio del cloud first

La conservazione dei dati della Pubblica Amministrazione avviene ormai solamente in formato digitale, in ossequio al principio *digital first.*

L'art. 40 del Codice dell'Amministrazione Digitale prevede che le PA formino gli originali dei propri documenti con mezzi informatici, e l'art. 43 chiarisce che gli obblighi di conservazione dei documenti si intendono soddisfatti a tutti gli effetti di legge con i documenti informatici, se conformi agli originali e alle linee guida.

Come ricordato nelle pagine precedenti, il CAD prevede la predisposizione di piani per la progressiva sostituzione degli archivi cartacei con quelli informatici. Di conseguenza ad oggi gli archivi cartacei sono sottoposti ad un regime che potremmo definire "ad

esaurimento". Ma a ben vedere, il citato articolo 42 del CAD collega tali determinazioni ad una valutazione sul rapporto tra costi e benefici e non indica un termine massimo per completare il passaggio dagli archivi cartacei a quelli digitali. Questa componente, lasciata alla valutazione discrezionale di ogni singola amministrazione ed unita alla mancanza del riferimento ad un termine ultimo per concludere lo *switch*, pare contribuire al rallentamento del processo di digitalizzazione della PA.

Svolta questa premessa, passiamo ora ad esaminare alcuni significativi interventi statali in tema di attuazione della Agenda digitale[44], che hanno inciso nella governance dei dati.

Una delle azioni trasversali della Strategia per la Crescita digitale del Paese prevede l'adozione progressiva del paradigma del *cloud computing*[45]. Il Piano Triennale per l'Informatica 2019-2021, in attuazione di questa scelta programmatica, contiene una decisa opzione per i servizi e le infrastrutture cloud. Tale opzione è stata consacrata con la enunciazione del principio *cloud first*[46].

Il PTI delinea un percorso di trasformazione dei sistemi informativi della PA, con l'obiettivo di passare dalla attuale frammentazione e disomogeneità ad una organizzazione evoluta ed efficiente.

Questa trasformazione dovrebbe poggiare su tre elementi-chiave: l'applicazione del già citato principio *cloud first* per la definizione di nuovi progetti e la programmazione di nuovi servizi delle PA; la progressiva migrazione delle infrastrutture e dei servizi esistenti verso il cloud (il c.d. *cloud enablement*); infine il potenziamento delle competenze mediante la creazione di Centri appositi, allo scopo di consolidare il *know-how* e l'esperienza relativa alla gestione dei servizi cloud nella PA.

Secondo quanto previsto nel PTI, tali Centri di competenza dovrebbero essere sorte di forum composti da tecnici, esperti e IT managers, *che discutano, propongano standard e regolamenti dei servizi digitali, condividano informazioni, soluzioni e competenze utili a mantenere, aggiornare, aumentare l'affidabilità dei sistemi*[47].

La strategia per l'adozione del *cloud computing* si sta realizzando anche attraverso vincoli alle spese per il settore ICT. Infatti, in attuazione del Piano Triennale 2019-2021, le PA non possono più effettuare investimenti su hardware e infrastrutture. Spese e investimenti potranno invece essere effettuati per progetti di virtualizzazione e per la migrazione dei servizi nelle infrastrutture del Cloud della PA.

Elemento non secondario, l'opzione per il *cloud computing* certamente risponde ad esigenze di riduzione dei costi per le infrastrutture informatiche[48], peraltro in aderenza a criteri di efficienza, efficacia ed economicità, richiamati anche nell'art. 12 del CAD[49].

Tale scelta a ben vedere, pare essere il fulcro di una più ampia strategia di razionalizzazione del patrimonio informativo della Pubblica Amministrazione[50]. Essa segna quindi una trasformazione culturale, prima che tecnica o giuridica, di non poco conto, se letta alla luce delle più volte richiamate dinamiche connesse alla digitalizzazione globale.

Su tale fronte, e prima di muovere verso la seconda questione relativa alla collocazione dei dati, ha un qualche rilievo citare il *Digital Economy and Society Index* (DESI), le cui risultanze sono state pubblicate l'11 giugno 2020[51]. Attraverso questo *Indice di digitalizzazione dell'economia e della società*, la Commissione Europea monitora il progresso digitale degli Stati membri dell'Unione.

Nel ranking complessivo viene indicata la sommatoria dei dati raccolti con riferimento a cinque aree tematiche: connettività, capitale umano, uso dei servizi internet, integrazione delle tecnologie digitali, servizi pubblici digitali. Il posizionamento dell'Italia al 25esimo posto su 28, nella sua eloquenza, stimola più di una riflessione[52].

Accanto a risultati soddisfacenti rispetto ad esempio alla connettività (in particolare alla "preparazione al 5G", ove l'Italia si colloca ben al di sopra della media europea), il DESI mette in luce carenze molto gravi per quanto riguarda il capitale umano, area nella quale l'Italia si colloca addirittura all'ultimo posto in Europa. Infatti solo il 42% degli individui di età compresa tra i 16 e i 74 anni possiede competenze digitali di base (rispetto alla media europea del 58%) e solo il 22% dispone di competenze digitali superiori a quelle di base (rispetto al 33% nell'Unione). L'uso modesto di internet, e la tipologia di contenuti oggetto delle ricerche online effettuate dagli utenti[53] sembrerebbero essere la diretta conseguenza delle scarse competenze digitali rilevate attraverso l'indagine europea.

Ciò nonostante, l'Indice europeo dà atto del crescente impegno dello Stato italiano per realizzare una efficiente digitalizzazione, impegno dimostrato tra l'altro attraverso l'istituzione del Ministero per l'innovazione tecnologica e la digitalizzazione, la presentazione della strategia *Italia 2025* e la predisposizione di un Piano Triennale per l'Informatica nella PA contenente un *elenco esaustivo di obiettivi per i prossimi anni.*

Tale impegno è comprovato dagli ottimi risultati conseguiti rispetto ai servizi pubblici online, ai servizi pubblici digitali per le imprese e all'open data, settori ove l'Italia supera persino il valore medio europeo. Tuttavia il dato, lungi dall'essere rassicurante,

è invece mortificante in quanto, nonostante i risultati appena citati, l'Italia si colloca al diciannovesimo posto nella classifica relativa ai servizi pubblici digitali. Il valore che inficia il risultato complessivo è quello relativo allo *scarso livello di interazione online tra le autorità pubbliche e il pubblico in generale. Solo il 32% degli utenti italiani online usufruisce attivamente dei servizi di e-government (rispetto alla media UE del 67%)*[54].

È appena il caso di sottolineare che un ritardo così grave non può che avere ripercussioni molto serie anche per la partecipazione del Paese al Mercato Unico Digitale. Tuttavia, la consapevolezza di queste gravi carenze, e soprattutto dello squilibrio tra lo sviluppo dei programmi di innovazione digitale delle PA e la scarsa attenzione ai diritti "digitali" di cittadini e imprese, così come garantiti dal CAD[55], potrebbe essere l'occasione per effettuare un investimento organico e strutturato sulla alfabetizzazione digitale[56]. Dunque il *digital divide*, se non affrontato in tempi rapidi, rischia di rivelarsi come l'ostacolo di gran lunga più difficile da rimuovere per la partecipazione dell'Italia al Digital Single Market[57].

Peraltro la diretta connessione tra *data literacy*, partecipazione alla economia digitale e sovranità tecnologica è un assunto della strategia digitale europea, confermato di recente nel White Paper sull'intelligenza artificiale[58].

6. Le regole di localizzazione: data storage pubblico e sovranità

Il secondo aspetto di rilievo in merito alla collocazione dei dati del settore pubblico riguarda la localizzazione fisica delle infrastrutture per la memorizzazione, in quanto talvolta la legge impone che determinati dataset siano conservati in server collocati sul territorio nazionale.

Anche in questo caso alcuni esempi saranno utili a chiarire i termini della questione.

La fattispecie più recente di imposizione di un obbligo di localizzazione in Italia può essere rinvenuta all'interno dell'art. 6 del d.l. n. 28 del 2020. Si tratta della norma sul *Sistema di allerta Covid-19*, che introduce una piattaforma per la gestione del sistema di tracciamento dei contagi ed impone che tale piattaforma sia localizzata sul territorio nazionale[59].

Come accennato nell'introduzione, il Garante per la protezione dei dati personali in fase di consultazioni aveva fatto una espressa raccomandazione in questo senso, richiamando il principio di precauzione in ragione della tipologia di dati oggetto di trattamento e quindi dei rischi elevati per i cittadini utenti della app di *contact tracing*[60].

Anche il Copasir, al termine di una attività di indagine e raccolta informazioni avviata in ragione di possibili rischi per la sicurezza nazionale, ha trasmesso al Parlamento una relazione sul sistema di allerta Covid-19[61]. Il Comitato, dopo aver richiamato l'esigenza che la conservazione dei dati avvenga sul territorio nazionale, esprime perplessità rispetto alla composizione della società proprietaria della app prescelta (Immuni). Infatti una quota minoritaria della Bending Spoons S.p.a. apparterrebbe ad un fondo riconducibile ad un uomo d'affari cinese. Le preoccupazioni espresse dal Copasir nascono in merito alla Cybersecurity law cinese, che *obbliga, in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità militari di pubblica sicurezza e alle agenzie di intelligence*[62].

Le conclusioni della Relazione divengono ancora più esplicite quando fanno espresso riferimento a rischi non trascurabili e non mitigabili sul piano geopolitico. Tali rischi sarebbero principalmente connessi alla necessaria e non fungibile presenza di partner privati non nazionali nella implementazione del sistema informatico di *contact tracing*; tali soggetti, ammonisce il Copasir, potrebbero manipolare i dati per finalità estranee da quella per la quale sono stati raccolti, di natura *politica, militare, sanitaria o commerciale*[63].

Un altro obbligo di localizzazione è contenuto nelle già richiamate Linee guida sulla formazione, gestione e conservazione dei documenti informatici, rilasciate dall'AgID in bozza per la consultazione. Nella sezione dedicata alle infrastrutture, vi è la prescrizione che i sistemi di conservazione delle PA e dei conservatori accreditati prevedano *la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale*, al fine di consentire all'Agenzia per l'Italia Digitale di svolgere le funzioni di vigilanza[64].

È utile ricordare che, secondo quanto precisato dal Consiglio di Stato, una volta adottate da AgID secondo la procedura indicata nell'art. 71 del CAD, le Linee guida acquisiranno carattere vincolante, assumeranno valenza erga omnes e saranno azionabili davanti al giudice amministrativo[65].

Proprio con riferimento alle regole di localizzazione dei dati, occorre qui mettere in evidenza una particolarità del sistema italiano. Infatti nella parte del Piano Triennale per l'Informatica nella PA dedicata al Cloud, più precisamente nella sezione delle domande frequenti, viene chiarito che vi è la possibilità per le PA di scegliere fornitori di servizi quali Google Cloud, Azure o altri providers, purché siano qualificati a norma della circolare Agid n. 3 del 9 aprile 2018, per la fruizione di servizi IaaS e PaaS[66].

I servizi di Cloud della tipologia *Infrastructure as a Service* possono fornire servizi di *computing*, *networking* e *storage* dei dati. La presenza nel Cloud Marketplace di AgID[67] di fornitori di servizi IaaS che non offrono all'utente la possibilità di scegliere la localizzazione dei siti ove verranno memorizzati e processati i dati, in controtendenza rispetto agli obblighi di localizzazione poc'anzi richiamati, sembra rivelare una lacuna nel coordinamento dei numerosi aspetti della complessa governance dei dati pubblici.

Accanto alle disposizioni normative e regolamentari appena richiamate, nei mesi scorsi il Garante per la protezione dei dati personali si è pronunciato ancora una volta in merito alla localizzazione dei dati personali, su impulso dell'Unione Camere Penali. Il riferimento è alla lettera inviata dal Presidente dell'Authority al Ministro della Giustizia Bonafede in merito ai software utilizzati per consentire lo svolgimento del processo penale da remoto[68]. Oggetto della richiesta di chiarimenti era la scelta, per la celebrazione delle udienze penali, di piattaforme fornite da un partner tecnologico (Microsoft) avente sede negli Stati Uniti, e per questa ragione soggetto all'applicazione del Cloud Act che *attribuisce alle autorità statunitensi un ampio potere acquisitivo di dati e informazioni*.

Gli obblighi di localizzazione imposti alle amministrazioni pubbliche italiane, unite ai richiami alle legislazioni cinese e statunitense, ci conducono al centro della questione.

Infatti come Vincenzo Zeno-Zencovich ha efficacemente sintetizzato commentando il Caso Schrems[69], *stabilire come i dati personali raccolti attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti ad altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto*[70].

Alcuni rapidi cenni alla normativa cinese sulla sicurezza cibernetica e a quella statunitense sul *cloud computing* permetteranno di mettere in luce le precise scelte strategiche volte a difendere la sovranità statale, entro (ed oltre) i limiti territoriali della propria giurisdizione.

Premettendo che l'articolatissimo sistema normativo e regolamentare della Repubblica Popolare Cinese in materia di privacy e sicurezza cibernetica[71], non è facilmente accessibile né decifrabile per uno studioso straniero, richiameremo nelle prossime righe solo alcuni tratti peculiari della governance cinese dei dati.

La *Cybersecurity law*[72], approvata nel novembre 2016, pone una serie di principi corredati in seguito da numerosissime integrazioni; si tratta di leggi, regolamenti, e standards che forniscono indicazioni tecniche per la implementazione del sistema nazionale di *cybersecurity*[73]. Questa legge, è importante sottolinearlo, non è incentrata sulla tutela dei dati personali (sebbene contenga delle norme a ciò dedicate), ma piuttosto sulla tutela della sovranità dello Stato, che viene assunta come la più alta priorità[74]. Il primo articolo elenca tra le finalità perseguite innanzitutto la salvaguardia della sicurezza cibernetica e della *cyberspace sovereignty*, per proseguire con la protezione dei diritti di cittadini e imprese e lo sviluppo della informatizzazione dell'economia e della società.

Gli operatori delle reti, principali destinatari delle regole previste dalla *Cybersecurity law*, debbono adeguare le loro infrastrutture ad una serie di requisiti tecnici finalizzati a garantire la sicurezza cibernetica. Gli obblighi saranno più o meno stringenti a seconda della tipologia di infrastruttura gestita[75]. Ai *network operators* è altresì esplicitamente fatto obbligo di collaborare con le autorità di pubblica sicurezza per la salvaguardia della sicurezza nazionale (art. 28).

Un interessante contributo di Aimin, Guosong e Wentong[76] articola il principio della sovranità cibernetica cinese in quattro diritti fondamentali: il diritto alla giurisdizione, cioè il diritto di gestire le reti informatiche presenti sul territorio nazionale; il diritto alla difesa contro gli attacchi informatici e le minacce esterne al Paese; il diritto alla indipendenza, ossia il diritto di usufruire dei servizi delle ICTs utilizzando esclusivamente network nazionali, indipendenti dal potere di altri Stati (il riferimento qui è al DNS statunitense); ultimo, il right of equality, che prevede per ogni Stato il diritto di avere giurisdizione sulle proprie reti informatiche[77].

Non a caso, uno degli strumenti normativi individuati dalla *Cybersecurity law* per affermare la propria sovranità cibernetica è l'imposizione agli operatori di *Critical Information Infrastructure*[78] dell'obbligo di localizzare i dati personali e gli *important data* da essi generati e raccolti, esclusivamente sul territorio nazionale[79].

Veniamo ora agli Stati Uniti, ove il Governo, dopo aver lanciato già nel 2011 la *Cloud First Strategy*, si appresta oggi a condurre una evoluzione dal paradigma *Cloud first* al *Cloud Smart*, basato su tre pilastri: *security*, *procurement*, e *workforce*[80]. Più rilevante rispetto all'oggetto del presente scritto è sicuramente la disciplina introdotta con il *Cloud Act*, relativa all'accesso da parte delle Autorità statunitensi a dati conservati al di fuori del territorio (e della giurisdizione) degli USA.

Infatti il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act*[81], approvato all'inizio del 2018, consente alle Autorità statunitensi di accedere alle in-

formazioni contenute nei server di *companies* statunitensi ovunque collocati nel mondo, al fine di garantire lo svolgimento di indagini e il perseguimento dei reati. Al contempo esso consente ai Governi stranieri di accedere, per le medesime finalità, a dati conservati sul territorio degli Stati Uniti. Il meccanismo si basa su un sistema di *executive agreements* negoziati bilateralmente con i singoli governi[82], che di fatto si sovrappone al modello, considerato inefficiente perché troppo lento e macchinoso, dei *Mutual Legal Assistance Treaties*[83].

Il fine dichiarato del Governo statunitense è quello di evitare conflitti di giurisdizione con altri Stati sovrani, e al contempo assicurare garanzie procedurali per tutti i casi di accesso ai dati personali.

Il risultato ottenuto, com'è noto, è molto controverso. Una parte dei commentatori ha sollevato dei dubbi sui rischi collegati ad una sensibile riduzione della protezione della privacy rispetto al precedente meccanismo dei MLATs. Altri sostengono invece che tale sistema sia completamente allineato con quello posto dal GDPR. Invero l'art. 48 del Regolamento europeo, disciplinando i trasferimenti non autorizzati di dati al di fuori dall'Unione europea nei casi in cui essi siano basati su una sentenza o una decisione amministrativa di uno Stato terzo, delinea una ipotesi di riconoscimento di tali atti proprio in presenza di un accordo internazionale, come un trattato di mutua assistenza giudiziaria[84].

A tale proposito è interessante notare come l'Unione europea si stia muovendo nella stessa direzione intrapresa dagli Stati Uniti per l'adozione di un Regolamento sull'accesso alle prove elettroniche, la cui proposta è attualmente in discussione in Consiglio[85], e la cui impostazione è in gran parte sovrapponibile al modello del Cloud Act.

Dalla sintetica analisi delle "strategie digitali" cinesi e statunitensi da ultimo proposta sembra di poter trarre una conferma del legame inscindibile tra data governance e affermazione della sovranità (digitale) dello Stato.

Basti ricordare che le scelte politiche cinesi e statunitensi di cui si è poc'anzi dato conto hanno avuto come conseguenza in primo luogo l'adozione, da parte degli altri Stati, di misure difensive del proprio patrimonio informativo; in secondo luogo, le grandi società fornitrici di servizi hanno dovuto adattarsi alle regole imposte per evitare di essere escluse da rilevantissime quote del mercato globale.

Non a caso, i big players hanno rapidamente provveduto a dotarsi di datacenters sul territorio della Repubblica Popolare cinese, e, sul fronte opposto, hanno elaborato soluzioni che, nel rispetto delle leggi, consentano di fatto ai loro clienti di sfuggire a possibili accessi indesiderati alle proprie informazioni da parte del Governo statunitense in forza del Cloud Act[86].

7. Riflessioni conclusive: la strategia digitale europea

La strategia europea si pone su un piano differente rispetto a tutto quanto sin qui descritto.

Infatti, a partire dal documento *A European Strategy for Data*[87] pubblicato il 19 febbraio 2020, viene presentata una visione dell'Unione europea nel contesto globale, che conferisce alla stessa una identità molto precisa, e la differenzia sensibilmente dagli altri attori mondiali.

Il documento, prese le mosse da una analisi dei ruoli degli USA e della Cina nella *data economy*, si prefigge di proporre/imporre una *European way*, che dovrebbe distinguersi per un bilanciamento, finora inedito, tra massimo utilizzo dei dati per lo sviluppo economico del Mercato Unico da una parte, e altissimi standard etici, di privacy, di safety and security dall'altra.

La grande novità proposta con la strategia europea è la creazione di *data spaces* tematici. Dalla possibilità di far circolare i dati ed estrarre da essi valore, innovazione, benefici per la collettività dipende l'espansione del Digital Single Market. La Commissione europea propone di realizzare questo effettivo cambio di marcia con un sistema di *pools* di dati, suddivisi in aree tematiche in modo che ogni settore possa trovare regole adeguate, e al contempo i singoli spaces possano comunicare tra di loro per massimizzare il flusso di dati, con il superamento dei limiti legati ai *data silos*.

L'Unione europea si appresta dunque a creare una grande area di localizzazione e scambio dei dati. Questa prospettiva introduce un ulteriore tema di tutt'altro che facile risoluzione: la governance dei flussi transfrontalieri di dati all'interno dell'Unione europea.

Come chiarito dal Considerando 5 del GDPR *L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. [...].*

Lo stesso dicasi per i flussi di dati non personali, ai quali è interamente dedicato il più volte citato Regolamento 2018/1807 FFD, il cui Considerando 10 recita eloquentemente: *A norma del regolamento*

(UE) 2016/679, gli Stati membri non possono limitare o vietare la libera circolazione dei dati personali all'interno dell'Unione per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento di dati personali. Il presente regolamento sancisce il medesimo principio di libera circolazione all'interno dell'Unione per i dati non personali [...]. Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati. [...][88].

Il combinato disposto dei due Regolamenti citati delinea dunque un modello di regolazione giuridica degli scambi di dati tra gli Stati membri, presupposto imprescindibile per lo sviluppo di una *data economy* dello spazio europeo.

La ritrosia degli Stati membri a considerare i servizi offerti e localizzati in altri Stati europei come facenti parte di un unico spazio giuridico, unita con un eccessivo protezionismo[89], ha portato ad una suddivisione delle banche dati nazionali in compartimenti stagni. Suddivisione che, come è evidente, ha sinora indebolito la posizione dell'Unione europea nell'economia globale.

Per contrastare questa tendenza l'Unione è impegnata nel rafforzamento di una visione comune che appare quanto mai necessaria alla tenuta e allo sviluppo del Mercato Unico Digitale. La scelta di contrastare le politiche nazionali di localizzazione, favorendo al contrario una apertura dei flussi tra Stati è condivisibile perché necessaria alla implementazione di una economia *data-driven*. Certamente il rafforzamento della fiducia rispetto alle modalità di trattamento dei dati e la chiara individuazione delle catene di responsabilità possono contribuire ad aumentare la fiducia e di conseguenza i flussi transfrontalieri di dati[90].

Tuttavia, sebbene il tema della fiducia sia di primaria importanza, vi è un dato strettamente giuridico che pare costituire la causa principale di questa disfunzione del sistema, ossia la frammentazione normativa che ancora differenzia sensibilmente le regole di trattamento dei dati. Questa realtà è stata bene messa in evidenza di recente nella relazione per i due anni di applicazione del GDPR[91]. In essa la Commissione denuncia quanto sia complesso sviluppare attività economiche/commerciali transfrontaliere, in particolare relative a tecnologie, innovazione e cybersecurity[92], a fronte di una ancora evidente differenziazione delle normative nazionali su aspetti di grande rilevanza pratica per le aziende, quali ad esempio il consenso dei minori in relazione ai servizi della società dell'informazione[93] e il regime di trattamento di particolari categorie di dati.

Peraltro la Commissione ha avuto l'occasione di richiamare gli Stati membri ad un "approccio paneuropeo", in stretto coordinamento per evitare la frammentazione, in sede di raccomandazioni per la gestione tecnologica della pandemia di Covid-19, con particolare riferimento alla gestione di situazioni di espansione transfrontaliera del contagio[94].

Tornando alla strategia dei *data spaces*, questa suddivisione per settori tematici dovrebbe contribuire a superare la descritta frammentazione, agevolando la condivisione di dati personali e non personali omogenei all'interno di aree regolamentate da norme comuni elaborate per quegli spazi. Nelle parole della Commissione: *Such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of common rules developed for the space*[95].

La Comunicazione, nella sua natura programmatica, non offre indicazioni specifiche sui passi che dovranno essere compiuti per la realizzazione di questo nuovo modello europeo di conservazione e condivisione dei dati. Significativamente però vengono annunciati, per il periodo 2021-2027, investimenti in un progetto ad alto impatto su spazi europei di dati e infrastrutture cloud federate.

Molto pragmaticamente la Commissione nel delineare i tratti principali della Strategia apre ad iniziative degli Stati membri per la realizzazione di infrastrutture comuni, annunciando la disponibilità ad elaborare protocolli d'intesa che favoriscano l'integrazione di tali iniziative nel progetto europeo[96].

Salta all'occhio, dato il tenore *high level* del documento, il riferimento esplicito al progetto franco-tedesco GAIA-X, che abbiamo citato nell'introduzione[97].

Occupiamoci brevemente di tratteggiare le caratteristiche distintive del progetto.

GAIA-X, nata da un'iniziativa del Governo tedesco, è divenuta ben presto oggetto di una partnership con la Francia, per poi essere presentata al resto dei Paesi dell'Unione europea con una conferenza di lancio che si è tenuta il 4 giugno 2020. Una volta realizzata, GAIA-X sarà una infrastruttura digitale *made in Europe*[98]. La sua ideazione ed il suo progressivo sviluppo sono il frutto della collaborazione di più di trecento partner pubblici e privati[99].

Da quanto è dato sapere, leggendo i documenti pubblicati in occasione del lancio del progetto, GAIA-X sarà un modulo di collegamento tra le infrastrutture di *cloud* ed *edge computing* nazionali. Così come per le infrastrutture, anche per quanto riguarda l'architettura giuridica è previsto che GAIA-X sia

disciplinata sulla base di principi, regole e standard già applicati nell'Unione europea[100].

L'infrastruttura sarà aperta alla partecipazione di attori pubblici e privati che rispettino quello che potremmo definire l'*acquis* di GAIA-X, ovvero l'insieme di principi e norme giuridiche e regole tecniche "europee" che l'iniziativa ha fatto proprie e che conta di arricchire con la progressiva elaborazione nuove policy e nuovi standard.

Di questo *acquis* fanno parte la protezione dati, la trasparenza, la fiducia, la sovranità sui dati, l'interoperabilità[101].

È bene a tal proposito evidenziare che all'interno di GAIA-X vengono utilizzati sia il termine *data sovereignty* che *digital sovereignty*[102]. Mentre la sovranità digitale viene definita come il potere di decidere *about how digital processes, infrastructures and the movement of data are structured, built and managed*, la *data sovreignty* viene presentata come un particolare aspetto della sovranità digitale, consistente nel pieno controllo del *data owner* rispetto alla collocazione e all'uso dei dati. La sovranità sui dati sarebbe dunque il primo passo per assicurare una sovranità digitale piena.

La finalità più volte richiamata nella documentazione rilasciata in occasione del lancio del progetto è di creare un ecosistema europeo per lo sviluppo della *data economy*[103]. GAIA-X si pone infatti come facilitatore dello sviluppo del mercato europeo dei dati[104]: nell'ecosistema di GAIA-X le imprese e le pubbliche amministrazioni dovrebbero sfruttare al massimo il potenziale dei dati, traendone servizi sempre migliori per la cittadinanza e sviluppo per il business delle imprese. Il tutto, entro i limiti della giurisdizione di almeno un Paese europeo.

GAIA-X sembra poter offrire una valida alternativa, seppure in gran parte ancora da costruire, alla dipendenza dell'Unione europea dai giganti tecnologici globali. Un ecosistema siffatto potrebbe rispondere alla richiesta di tutela dei diritti dei cittadini/utenti, favorire lo sviluppo della *data economy* a livelli davvero competitivi, e infine potrebbe garantire la sovranità digitale degli Stati membri dell'Unione europea. Alcuni punti però dovranno certamente essere chiariti nelle fasi di implementazione.

Ad esempio, vale la pena di precisare che ogni provider che entrerà a far parte dell'infrastruttura, resterà responsabile per il servizio da esso prestato[105]: *GAIA-X is a federated system of autonomous providers [. . .]. In accordance to the shared responsibility model each GAIA-X Partecipant is responsible for the service and data which is controlled by him.* Nei documenti pubblicati si legge anche che legittimamente un Consumer potrebbe richiedere una prova della reale localizzazione dei propri dati, rispetto a quanto garantito dal provider.

Dunque, privata dell'enfasi del lancio del progetto e dell'entusiasmo legato alla totale adesione alla strategia europea, GAIA-X si presenta come un sistema di collegamento tra server nazionali situati nel territorio dell'Unione. Una rete di *mutual agreements* consentirà di avere la certezza giuridica che tutti i partecipanti al progetto GAIA-X rispondano agli stessi requisiti tecnici e valoriali. Per la verifica della compliance al GDPR viene proposto l'utilizzo di certificazioni e codici di condotta a norma degli artt. 40 e 42 del Regolamento europeo[106].

Tale riferimento appare particolarmente adeguato e strategico, nell'ottica dell'efficienza del sistema e ancor di più nell'ottica dello sviluppo e rafforzamento dello spazio digitale europeo. Nella sistematica del GDPR l'elaborazione di codici di condotta dovrebbe contribuire alla corretta applicazione del Regolamento medesimo in settori specifici[107], mentre le certificazioni, i sigilli e i marchi dovrebbero servire a dimostrare la conformità al GDPR dei trattamenti svolti nella fornitura di prodotti e servizi[108].

L'articolo 40, relativo ai codici di condotta, prevede che il progetto di codice debba essere presentato dalle associazioni o altri organismi di rappresentanza di titolari e responsabili alla Autorità di controllo competente, ovvero quella dello Stato ove i richiedenti abbiano la sede legale. Se le attività si svolgono interamente nel territorio dello Stato di cui si trova l'associazione, l'Autorità competente potrà autonomamente procedere alla approvazione del codice di condotta.

Ma ciò che davvero rileva, rispetto all'argomento che ci occupa, è la procedura prevista dai paragrafi 7 e seguenti del medesimo articolo, relativa alle ipotesi di flussi transfrontalieri di dati. Infatti quando il progetto di codice di condotta si riferisce ad attività di trattamento che interessano diversi Stati membri, l'Autorità di controllo compente è tenuta, in ossequio al meccanismo di coerenza, a sottoporre il progetto al Comitato europeo per la protezione dei dati personali (EDPB). Il Comitato formulerà un parere che sarà poi trasmesso (in caso di valutazione positiva sulla conformità al GDPR) alla Commissione. Quest'ultima poi con un atto di esecuzione conferirà al codice di condotta validità generale su tutto il territorio dell'Unione.

Certificazioni, marchi e sigilli, possono essere rilasciati, a norma dell'art. 42, dalle Autorità di controllo, da organismi di certificazione o dal Comitato europeo (EDPB). Quest'ultimo ha il potere di approvare dei criteri di certificazione che consentano poi a titolari e responsabili del trattamento di otte-

nere un sigillo europeo. Anche in questo caso sono le Autorità di controllo ad individuare i criteri per la certificazione. La Commissione ha il potere, a norma dell'art. 43, di precisare i requisiti di cui tener conto delle certificazioni, oltre che di stabilire norme tecniche riguardanti tali meccanismi e la promozione degli stessi.

Dunque, come è stato autorevolmente evidenziato[109], nella produzione di codici di condotta e certificazioni le Autorità di controllo nazionali svolgono una funzione di primaria importanza. Non solo, in alcuni settori specifici, il GDPR prevede un intervento dell'European Data Protection Board per il controllo e il coordinamento delle Autorità nazionali coinvolte.

Posto l'ecosistema di riferimento, gli organi investiti dei poteri di regolazione e controllo, coordinati grazie ai meccanismi di cooperazione e coerenza, potranno contribuire alla creazione di regole condivise (tra cui i codici di condotta europei) che gradualmente condurranno alla realizzazione di uno spazio giuridico sicuro dal punto di vista delle tutele dei diritti fondamentali e funzionale allo sviluppo della *data economy*[110].

A sostegno di questa tesi deve essere ricordato, inoltre, che l'art. 64 par. 2 prevede che il Comitato europeo si pronunci su questioni di applicazione generale o relative a più Stati membri. Questo ruolo appare di importanza strategica per il progressivo consolidamento della *data governance* europea. Non a caso l'articolo 70 del GDPR individua nella garanzia dell'applicazione coerente del Regolamento la prima determinante funzione dell'EDPB.

Il ruolo appena tratteggiato delle Autorità di controllo, della Commissione e del European Data Protection Board nel consolidamento del Mercato Unico assume ancora più rilievo alla luce della possibilità offerta dal Regolamento a titolari e responsabili non soggetti al GDPR di aderire a codici di condotta e certificazioni nel quadro di trasferimenti di dati personali presso paesi terzi o organizzazioni internazionali.

A ben vedere la progressiva edificazione di un apparato regolamentare agile ed efficiente potrebbe essere la cifra distintiva della *(big) data governance* del settore pubblico attraverso la quale l'Unione potrà riaffermare (e tutelare) la sovranità europea sui dati nello scacchiere digitale globale.

Note

[1]The Guardian, *UK government told not to use Zoom because of China fears*, 24 April 2020.

[2]Divenuta popolarissima a seguito delle misure di isolamento e distanziamento sociale dovute al contenimento della pandemia di Covid-19. Il tema principale della presente ricerca non è strettamente connesso alla pandemia. Tuttavia, nello scritto si farà più volte riferimento ad atti, documenti, decisioni che sono correlati alla pandemia medesima, assumendo che il contesto della emergenza sanitaria globale dichiarata dall'Organizzazione Mondiale della Sanità il 30 gennaio 2020 sia noto ai lettori.

[3]Già da inizio aprile 2020 infatti un centro studi dell'Università di Toronto aveva evidenziato le debolezze del sistema di crittografia utilizzato dalla piattaforma e i rischi derivanti dal fatto che le chiavi di sicurezza fornite ai partecipanti agli Zoom meetings venissero inviate da server collocati in Cina: «An app with easily-identifiable limitations in cryptography, security issues, and offshore servers located in China which handle meeting keys presents a clear target to reasonably well-resourced nation state attackers, including the People's Republic of China». Cfr. B. Markzar, J. Scott-Railton, Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings, The citizen lab, University of Toronto, 3 aprile 2020.

[4]Cfr. *German government's digital summit*, 29 October 2019.

[5]Cfr. la posizione comune del 18 febbraio 2020.

[6]La presentazione ufficiale del progetto è avvenuta il 4 giugno 2020 con un evento promosso dal *German Federal Ministry for Economic Affairs and Energy*.

[7]Garante per la protezione dei dati personali, *Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro datadriven per l'emergenza COVID-19*, 7 aprile 2020.

[8]Richiesta peraltro esaudita, come risulta dal d.l. n. 28/2020 in cui all'art. 6, relativo al sistema di tracciamento, si specifica che la piattaforma unica nazionale di gestione del sistema di allerta costituenda sarà realizzata "esclusivamente con infrastrutture localizzate sul territorio nazionale".

[9]Cfr. il testo completo dell'intervista.

[10]O. Pollicino, *L'"autunno caldo" della corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "Federalismi.it", 16 ottobre 2019.

[11]Si tratta delle decisioni: Corte di giustizia dell'Unione europea, sentenza C-507/17, *Google LLC contro Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019; Corte di giustizia dell'Unione europea, sentenza C-18/18, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*, 3 ottobre 2019.

[12]Per l'analisi dei due casi si rinvia a O. Pollicino, *op. cit.*

[13]«Se ci terremo ad una tradizione [...] per cui il diritto è fatto, il fatto della volontà di chi ha la forza, e continueremo a fondarlo sulla sovranità, avremo un bel da fare a comprendere e governare un presente in cui la sovranità riesce sconfitta (per non fare che un esempio) da un giovanotto intelligente e pratico di computer. [...] Siamo stati abituati a pensare per duecento anni che la sovranità fosse la base del diritto. Proviamo ora a pensare che il diritto sia la base della sovranità», A. Gentili, *La sovranità nei sistemi giuridici aperti*, in "Politica del diritto", giugno 2011, n. 2, p. 205.

[14]Per una descrizione efficace dei rischi e delle potenzialità legati alla Big data analytics si veda S. Calzolaio, voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017, p. 594 ss.; su Big Data e machine learning, A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1, pp. 87-106.

[15]Basti scorrere l'elenco delle Basi di dati di interesse nazionale, all'art. 60 del Codice dell'Amministrazione Digitale (CAD), d.lgs. n. 82/2005.

[16]Le definizioni di queste categorie sono contenute negli artt. 4 e 9 del Regolamento europeo sulla protezione dei dati personali (UE) 2016/679 (*General Data Protection Regulation*) e nell'art. 3 del Regolamento europeo sulla libera circolazione dei dati non personali (UE) 2018/1807 (*Free Flow Data Regulation*).

[17]S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in "Giornale di storia costituzionale", 2016, n. 31, p. 198.

[18]AGID, *Piano Triennale per l'Informatica 2019-2021.*

[19]Nel Piano Triennale 2019-2021 i limiti del paradigma Smart city, che hanno portato alla evoluzione nel modello Smart landscape sono descritti così: «Le iniziative finora condotte sul tema, in particolare da alcune città metropolitane, per quanto apprezzabili, sono però accomunate da un approccio limitato al contesto urbano di riferimento e quasi tutte prendono in maggior considerazione gli aspetti correlati al "cittadino" tralasciando quelli che hanno un forte impatto sulle imprese, quali, ad esempio, il movimento delle merci e le opportunità derivanti dalle integrazioni con altri sottosistemi (Port Communities, Cargo communities, nodi logistici territoriali, imprese di distribuzione...). [...] La logistica rappresenta un settore strategico per l'economia nazionale da considerare strumento di politica industriale, per valorizzare le eccellenze del sistema produttivo e per promuovere lo sviluppo del trasporto ecosostenibile e la tutela dell'ambiente. La declinazione del paradigma "Internet of Things" applicato alle merci implica l'integrazione dei servizi resi da differenti attori pubblici/privati che si può ottenere grazie ad una completa digitalizzazione della catena logistica. Soluzioni intelligenti, "smart", basate sull'utilizzo di corridoi e nodi logistici interconnessi, consentono di dominare la complessità in questo settore - legata anche al carattere multimodale del trasporto e alla pluralità di attori coinvolti – e di recuperare notevoli spazi di efficienza, ottimizzando i tempi ed i costi di spostamento delle merci, garantendo safety e security. L'attenzione va quindi rivolta ad un sistema ampio e complesso, che comprende anche una pluralità di "nodi logistici "(porti, aeroporti, retroporti, interporti, piattaforme logistiche territoriali, centri e aziende di distribuzione ...) e dai collegamenti intermodali tra essi, necessari a rendere funzionale l'ambito logistico nel complesso, da tutti i nodi logistici e dalle città, perseguendo, attraverso un approccio sinergico, coordinato e integrato, un'ottica di ottimizzazione degli investimenti e di efficienza e lo sviluppo di sinergie di sistema, attuando una "logistica sostenibile" (sostenibilità economica, ambientale, sociale). [...] I programmi nazionali attivati e in via di attivazione dovrebbero essere quindi sinergicamente inquadrati in un'ottica più ampia per rendere interoperabili le soluzioni verticali sviluppate al fine di pervenire ad una gestione intelligente e sicura della mobilità, delle persone e delle merci, favorendo lo sviluppo di servizi basati sulle esigenze dei cittadini e delle imprese». Appare dunque evidente la spinta verso un modello integrato di servizi alla persona e servizi all'impresa/logistica.

[20]L'art. 50 del CAD prevede già la possibilità per le PA, nell'ambito delle proprie funzioni istituzionali, di procedere all'analisi dei dati, anche in combinazione con quelli detenuti da altre PA, da gestori di servizi pubblici e da società a controllo pubblico, escluse quelle quotate che non gestiscano servizi pubblici.

[21]Su questo tema sia consentito rinviare a V. Pagnanelli, *Accesso, accessibilità, Open data. Il modello italiano di Open data pubblico nel contesto europeo*, in "Giornale di storia costituzionale", 2016, n. 31, p. 205 ss.

[22]Si veda in proposito F. Sciacchitano, *Disciplina e utilizzo degli Open Data in Italia*, in "Medialaws", 2018, n. 1, p. 281 ss.

[23]S. Calzolaio, voce *Protezione dei dati personali*, cit., p. 601.

[24]Il modello di gestione della pandemia della Regione Veneto, pur nella complessità delle questioni giuridiche che ha sollevato e che non possono essere trattate in questa sede, pare essere stato, almeno in una prima fase, un esempio di utilizzo efficace delle banche dati nel contenimento dell'emergenza sanitaria.

[25]A titolo di esempio, sull'utilizzo delle tecniche di *Deep fake* si veda F. Bertoni, *Deepfake, ovvero Manipula et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in "Ciberspazio e diritto", 2019, n. 1-2, pp. 11-28.

[26]Sulle potenzialità ed i rischi dell'utilizzo dei *Big Data* nel settore pubblico si veda G.M. Ruotolo, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in Studi sull'integrazione europea, 2018, n. 3, p.105 ss.; più in generale, su opportunità e rischi della democrazia al "tempo del digitale", P. Costanzo, *La democrazia digitale (precauzioni per l'uso)*, in "Diritto pubblico", 2019, n. 1.

[27]Autorità garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, documento finale, 10 febbraio 2020.

[28]*Ivi*, pp. 68-69.

[29]Per tutti, G. D'Acquisto, M. Naldi, *Big data e privacy by design*, Giappichelli, 2017, in particolare Cap. 1, *Big Data e protezione dei dati personali.*

[30]Autorità per le Garanzie nelle Comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 14.

[31]Cfr. *Ibidem*, *Executive Summary*, p. 7.

[32]L'articolo 3 n. 1 del Reg. n. 2018/1807 definisce i dati come «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del Regolamento (UE) n. 2016/679».

[33]L'art. 8 dello stesso articolato, che prevede la elaborazione da parte della Commissione, entro il 29 novembre 2022, di una relazione sull'attuazione del Regolamento e in particolare sugli insiemi misti di dati personali e non personali in ragione dei futuri progressi tecnologici non prevedibili, sembra confermare le perplessità.

[34]Regolamento n. 2018/1807, art. 3 n. 2.

[35]Le regole contenute nei massimari di conservazione e scarto ed il vaglio della Sovraintendenza archivistica definiscono ulteriormente il quadro di gestione degli archivi pubblici.

[36]Il titolare del trattamento è la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che determina finalità e mezzi del trattamento dei dati personali (GDPR, art. 4 n. 7).

[37]Cioè la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare (GDPR, art. 4 n. 8).

[38]A solo titolo di esempio, l'esito dell'attività di scarto nell'archivio cartaceo comporterà la distruzione materiale dei documenti attraverso invio al macero, da affidarsi a imprese specializzate in tale senso; la medesima attività si svolgerà con modalità ovviamente differenti presso gli archivi digitali.

[39]Cfr. d.lgs. n. 82/2005, art. 42.

[40]«[...] la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del trattamento», GDPR, art. 28 par. 3.

[41]Il riferimento è all'art. 17 bis del decreto c.d. "Cura Italia" (d.l. 17 marzo 2020, n. 18 conv. con legge 24 aprile 2020, n. 27) in cui viene elencata una lunga serie di soggetti che al fine di poter gestire e contenere l'emergenza sanitaria da Covid-19

sono autorizzati a trattare dati anche relativi agli articoli 9 e 10 del GDPR e a farne oggetto di comunicazione.

[42] Cfr. la bozza delle Linee guida.

[43] Garante per la protezione dei dati personali, *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, 13 febbraio 2020.

[44] «Lo scopo dell'Agenda Digitale è fare leva sul potenziale delle tecnologie ICT per favorire innovazione, progresso e crescita economica, avendo come obiettivo principale lo sviluppo del mercato unico digitale. Nel quadro dell'Agenda Digitale Europea, l'Italia ha sviluppato l'Agenda Digitale Italiana, una strategia nazionale per raggiungere gli obiettivi indicati dall'Agenda Europea». Cfr. l'Agenda Digitale.

[45] Presidenza del Consiglio dei Ministri, *Strategia per la crescita digitale 2014-2020*, 21 giugno 2016, p. 61.

[46] «In base al principio Cloud First, le PA in fase di definizione di un nuovo progetto, e/o sviluppo di nuovi servizi, devono, in via prioritaria, adottare il paradigma cloud in particolare i servizi SaaS, prima di qualsiasi altra opzione tecnologica». Cfr. *Il cloud enablement*.

[47] *Ibidem*.

[48] «Le applicazioni cloud (SaaS) si pagano generalmente in base al consumo, consentono di gestire la crescita di un servizio in maniera dinamica e richiedono investimenti iniziali estremamente limitati. [...] Il ridotto investimento iniziale implica una riduzione del rischio, è così possibile sviluppare e testare, su scala ridotta, soluzioni che possono essere valutate velocemente per poi essere adottate, modificate radicalmente o abbandonate, con costi minimi». Cfr. *Perché usare il cloud*.

[49] «Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione [...]». Si veda in proposito A. Masucci, *Digitalizzazione dell'amministrazione e servizi pubblici online. Lineamenti del disegno normativo*, in Diritto Pubblico, 2019, n. 1, p. 140 ss.

[50] Razionalizzazione significativamente basata sul coordinamento informatico a livello centrale. A norma dell'art. 14 del CAD «L'AgID assicura il coordinamento informatico dell'amministrazione statale, regionale e locale [...]». Sul punto M. Di Francesco Torregrossa, *La competenza statale nel processo di digitalizzazione delle pubbliche amministrazioni*, in Consulta online, 2019, n. 1, p. 64 ss.

[51] Cfr. *Le performance digitali di tutti i Paesi dell'UE*.

[52] Cfr. *Lo scoreboard italiano*.

[53] Il 79% degli utenti utilizza internet per fruire di musica, video e giochi.

[54] V. *supra* nota 49, p. 14.

[55] L'art. 3 riconosce a chiunque il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti previsti dal CAD nei rapporti con le amministrazioni pubbliche.

[56] Come prescritto dall'art. 8 del CAD.

[57] Sul ruolo-chiave della *digital literacy* per lo sviluppo del Mercato Unico Digitale cfr. V. Pagnanelli, *op. cit.*, p. 212: «L'evoluzione rapida e irreversibile verso l'amministrazione digitale pone tra le priorità assolute il superamento del *digital divide*, e di conseguenza i passi da compiere in quella direzione. Tra di essi un serio investimento sulla *digital literacy* appare ormai necessario».

[58] «Lo sfruttamento della capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione nonché nelle competenze digitali, come l'alfabetizzazione ai dati (data literacy), accrescerà la sovranità tecnologica dell'Europa nell'ambito delle tecnologie e infrastrutture abilitanti fondamentali per l'economia dei dati». Commissione europea, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, 19 febbraio 2020, p. 4.

[59] A norma dell'art. 6, la piattaforma unica nazionale per la gestione del sistema di allerta «è di titolarità pubblica ed è realizzata [...] esclusivamente con infrastrutture localizzate sul territorio nazionale».

[60] Cfr. *supra* nota 5.

[61] Comitato parlamentare per la sicurezza della Repubblica (COPASIR), *Relazione sui profili di sicurezza del sistema di allerta Covid-19 previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020*, 13 maggio 2020.

[62] *Ivi*, p. 11.

[63] *Ivi*, p. 13.

[64] Garante per la protezione dei dati personali, *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, cit.

[65] *Ivi*, Capitolo 1.10.

[66] Vedi la *Circolare qualificazione cloud service provider*; per una analisi dei modelli Cloud e delle diverse tipologie di servizi forniti si rimanda interamente al contributo di Vanni Boncinelli, in questo fascicolo.

[67] Vedi *AGID Cloud Marketplace*.

[68] Garante per la protezione dei dati personali, *Processo penale da remoto: lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro della Giustizia, Alfonso Bonafede*, 16 aprile 2020.

[69] La notissima sentenza con cui la Corte di Giustizia UE ha dichiarato l'invalidità della decisione della Commissione UE n. 2000/252/CE sull'accordo denominato Safe Harbour relativo al trasferimento dei dati personali di cittadini europei verso gli USA. Sul caso Schrems si vedano, *ex plurimis* G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai «Safe Harbour Principles» al «Privacy Shield»", Tre Press, 2016, pp. 23-48; M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in "Rivista AIC", 2016, n. 3; V. Fiorillo, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in "Federalismi.it", 26 luglio 2017. Un nuovo capitolo della vicenda è stato scritto di recente con la pubblicazione il 16 luglio 2020 della sentenza nella causa C-311/18 *Data Protection Commissioner / Maximilian Schrems e Facebook Ireland*, con la quale la Corte di Giustizia UE ha dichiarato l'invalidità della decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del c.d. Privacy Shield EU-US per il trasferimento di dati personali verso gli Stati Uniti (sentenza pubblicata quanto il presente articolo era già in bozze e quindi citata solo nei riferimenti essenziali).

[70] V. Zeno Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta, V. Zeno Zencovich (a cura di), "op. cit.", p. 11.

[71] Per una contestualizzazione G. Greenleaf, *Asian data privacy law. Trade and Human rights perspectives*, Oxford University Press, 2014, p. 192 ss.; J.R. Lindsay, T.M. Cheung, D.S. Reveron, *China and cybersecurity espionage, strategy and politics in the digital domain*, Oxford University Press, 2015, in particolare, Cap. 10; G. Austin, *Cybersecurity in China. The next wave*, Springer, 2018.

[72] Per una analisi del contenuto della *Cybersecurity Law* si vedano L. Huang, D. Ilan, K. Mooney Carrol, Z. Zhou, *Understanding the impact of China's far-reaching new Cybersecurity law*, in "Intellectual Property & Technology Law Jour-

nal", 2018, n. 2, p. 15 ss.; Q. Aimin, S. Guosong, Z. Wentong, *Assessing China's cybersecurity law*, in "Computer Law & Security Review", 2018, n. 34, p. 1342 ss.

[73] *National standards* e *technical guidances* sono ulteriormente suddivisi per tipologia in *mandatory standards* (GB Standards), *voluntary standards* (GB/T Standards) *and technical guidance* (GB/Z guidance).

[74] Cfr. Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*, p. 1344. L'Italia si è dotata della propria *cybersecurity law* con il d.l. 21 settembre 2019 n. 105, conv. con l. 18 novembre 2019 n. 133, che ha istituito il perimetro di sicurezza nazionale cibernetica.

[75] La legge cinese prevede una disciplina "aggravata" per gli operatori di *Critical Information Infrastructure*, definite come «infrastructure that is used in public communications and information services, energy, transportation, water conservancy, finance, public services or electronic governance or that, if it were destroyed, malfunctioned or leaked data, could seriously endanger national security, national welfare and the people's livelihood, or the public interest»; cfr. L. Huang, D. Ilan, K. Mooney Carrol, Z. Zhou, *op. cit.*, p. 17 ss.

[76] Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*

[77] *Ivi*, pp. 1345-1346.

[78] Cfr. *supra* nota 73.

[79] «Specifically, the data required to be stored locally in accordance with other laws or regulations include: population and Health data (Section 10 of the Provisional Measures on Population health Information Management), credit information (Section 24 of the Rules on Credit Industry Administration), personal financial information (Article 6 of the People's Bank of China Notice on the Protection of Personal Financial Information), map data (Section 34 of the Rules on Map Management), online publication data (Article 8 of the Regulations on the Administration of Online Publishing Services); data related to online car-hailing business (Article 27 of the Provisional Measures on Online Car-hailing Operation Service Management)»; cfr. Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*, p. 1351.

[80] Cfr. la *Federal Cloud Computing Strategy*.

[81] Cfr. il testo del *Cloud Act*; il *White paper* pubblicato dal U.S. Department of Justice nell'aprile 2019 ne descrive *background*, caratteristiche e finalità.

[82] Cfr. *Cloud Act*, Sec. 105. *Executive agreements on access to data by foreign governments*, nella quale sono elencati i requisiti che il Governo straniero deve possedere per poter sottoscrivere un accordo bilaterale.

[83] «A long-established way for the U.S. government to access private information held abroad is through Mutual Legal Assistance Treaties. These agreements permit a public authority seeking data to ask for the assistance of the country in which the data is held and require that country to cooperate in processing such requests under its domestic law. MLATs establish legal mechanisms for cooperation between signatory nations in criminal matters and proceedings, including the exchange of evidence and information during criminal proceedings», P.M. Schwarts, *Legal access to the global cloud*, in Columbia Law Review, 2018, n. 6, p. 1720.

[84] Sulle criticità del meccanismo introdotto dal *Cloud Act* si veda H.H. Abraha, *How compatible il the US "Cloud Act" with cloud computing? A brief analysis*, in International Data Privacy Law, 2019, n. 3, p. 207 ss.; *contra* M.W. Brennan, W. Maxwell, A.A. Sura, *Demistifying the Cloud Act: assessing the law's compatibility with international norms and the GDPR*, Hogan Lovells, January 2019, i quali sostengono che le garanzie introdotte dal *Cloud Act* siano adeguate agli standard internazionali in materia di protezione dati, compreso il GDPR.

[85] Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* - COM/2018/225 final 2018/0108 (COD).

[86] Il *Data Trustee model* elaborato da Microsoft per il mercato tedesco costituisce un esempio di tali soluzioni. In proposito cfr. H.H. Abraha, *op. cit.*, p. 208: «This arrangement [the Data trustee model, N.d.A.] could create a situation where personal data concerning a US person and required for US domestic crime investigation purpose is neither located in the USA nor effectively controlled by a US company». Il modello *Data trustee* elaborato da Microsoft consente alla *company* di mantenere la responsabilità sul servizio dal punto di vista tecnico, rispettando allo stesso tempo la esigenza di localizzazione dei dati sul territorio tedesco, in modo che gli stessi siano esclusivamente sottoposti alla legislazione tedesca. Il *trustee* tedesco e l'interessato potranno accedere ai dati, mentre Microsoft potrà farlo solo in limitati casi previsti dal contratto.

[87] *European Commission*, *Communication from the Commission to the European Parliament, The Council, The European economic and social Committee and the Committee of the Regions. "A European strategy for data"* - COM(2020) 66 final, 19 febbraio 2020.

[88] L'articolo 4 del Regolamento FFD vieta agli Stati di imporre obblighi di localizzazione che impongano di effettuare il trattamento sul territorio dello Stato o ostacolino il trattamento in un altro Stato membro. Per una disamina approfondita delle regole sulla circolazione dei dati nell'ordinamento europeo si rimanda al contributo di Stefano Torregiani, in questo fascicolo.

[89] Il Copasir, nell'esprimere preoccupazione rispetto ad usi malevoli dei dati conservati al di fuori del territorio italiano, ha fatto esplicito riferimento ad "attori europei ed internazionali" che possano a vario titolo essere interessati alle informazioni raccolte, lasciando trasparire la mancanza di una visione in tema di spazio comune europeo dei dati.

[90] Il Considerando 7 del GDPR fa riferimento all'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. Franco Pizzetti lo definisce «principio di fiducia, che deve essere assunto come criterio interpretativo di base e come l'obiettivo ultimo che giustifica anche la stretta connessione fatta dall'art. 1 GDPR tra l'attuazione del diritto fondamentale alla tutela dei dati e la necessità di garantirne la libera circolazione»; cfr. F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 170.

[91] European Commission, *Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation* - COM(2020) 264 final, 24 giugno 2020.

[92] Cfr. *Ivi*, p. 7.

[93] Il GDPR lascia agli Stati la possibilità di stabilire un'età inferiore a sedici anni (opportunità colta per esempio dall'Italia, che con l'art. 2 *quinquies* del Codice della Privacy novellato ha abbassato la soglia a quattordici anni).

[94] European Commission, *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*.

[95] European Commission, *Communication from the Commission to the European Parliament, The Council, The European economic and social Committee and the Committee of the Regions. "A European strategy for data"*, cit., p. 16.

[96] *Ivi*, p. 18.

[97] *Supra* par. 1.

[98] *GAIA-X: The European project kicks off the next phase*, June, 2020, p. 2.

[99] Tra di essi anche Google Germany GmbH.

[100] Su portabilità, interoperabilità, interconnessione tra infrastrutture, applicazioni, dati.

[101] Il documento *GAIA-X: Policy Rules and Architecture of Standards*, June 2020, richiamando la posizione Franco-tedesca li individua in: «1. European data protection 2. Open-ness, reversibility, and transparency 3. Authenticity and trust 4. Digital sovereignty and self-determination 5. Free market access and European value creation 6. Modularity and interoperability 7. Federation of infrastructure».

[102] GAIA-X: Technical Architecture, June 2020, p. 3.

[103] «GAIA-X combines the technological and industrial strengths of EU industry, academia and the public sector to develop an ecosystem of data and infrastructure providers and a regulatory framework based on fundamental European values and standards. The initiative supports the target of the EU to be-come a global leader in innovation in the data economy and its data-driven applications as set out in the European data strategy»; *GAIA-X: Driver of digital innovation in Europe*, May 2020, p. 25

[104] *Ivi*, p. 39.

[105] *GAIA-X: Technical Architecture*, cit., p. 30.

[106] *Ivi*, p. 32.

[107] Il Considerando 99 del GDPR specifica che i codici di condotta dovrebbero facilitare l'applicazione del regolamento «tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese».

[108] Cfr. Considerando 100 del GDPR, secondo cui certificazioni, sigilli e marchi dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati offerto da tali prodotti e servizi.

[109] F. Pizzetti, *op. cit.*, p. 175 ss.

[110] In particolare le certificazioni, strumenti chiaramente elaborati per essere impiegati a livello europeo, potranno essere utilizzati dalle Autorità nazionali, dall'EDBD e dalla Commissione per agevolare la circolazione dei dati nello spazio digitale dell'Unione. Pizzetti sottolinea le differenze di formulazione degli articoli 40 e 42, che lungi dall'esser solo formali, evidenziano una spiccata opzione per le certificazioni di validità europea. Cfr. F. Pizzetti, *op. cit.*, p. 157 e p. 160.

* * *

Data storage and digital sovereignty: The public (big) data governance facing the new global challenges

Abstract: By using data retention policies in the public sector as a paradigm, the paper reflects on how States are asserting or defending their digital sovereignty. The article recalls the digitization path of the Italian PA, on which big data has had a significant impact. The digital data storage has imposed the transition from paper archives to the cloud, a transition regulated by national and European legislation and partly influenced by the digital strategies of the great world powers. The proliferation of localization obligations and prohibitions confirms the complexity and centrality of these issues in the protection of digital sovereignty. The paper ends with an analysis of the key points of the *European strategy for data* published by the European Commission in February 2020, and with a look at the Franco-German data storage and data sharing project called GAIA-X.

Keywords: Data storage – Digital sovereignty – Public sector – Data localization

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0023

Modelli tecnici e disciplina giuridica del c.d. cloud computing

Vanni Boncinelli

Il mercato dei servizi di *cloud computing* ha registrato negli ultimi anni uno tasso di crescita esponenziale, che la recente emergenza sanitaria mondiale finirà per rafforzare ulteriormente. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione "sinergica" di fattori, nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha portato a nuove modalità di utilizzo dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, i quali non potrebbero esistere (o quasi) senza le risorse computazionali, applicative e di *storage* messe a disposizione da fornitori di *cloud computing*. Dal punto di vista giuridico, tuttavia, il *cloud computing* lascia sul tappeto enormi interrogativi ancora in gran parte irrisolti. Come proteggere i diritti degli interessati quando i loro dati possono essere spostati, spacchettati, ricomposti e replicati in qualsiasi nodo della rete globale con un semplice click? Come regolare un caleidoscopio di servizi così diversi tra loro e ripartire obblighi e responsabilità tra i vari soggetti che compongono la "filiera" *cloud*? Per molti versi, l'approccio seguito da Stati Uniti e Unione europea non potrebbe essere più diverso, ma entrambi scontano la pretesa di voler regolare in modo unilaterale un fenomeno – il *cloud computing* e, più in generale, Internet – nel quale "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Cloud computing – Cloud Act – e-Evidence Regulation

Sommario: *1. Introduzione – 2. Un* cloud*, mille* cloud*. Genesi, evoluzione e caratteristiche del* cloud computing *– 3. I principali modelli di servizio – 4. I modelli di distribuzione del* cloud computing *– 5. Una classificazione alternativa dei servizi* cloud*:* Data Shard*,* Data Localization*,* Data Trust *– 6. L'approccio al* cloud *al di là dell'oceano: i casi* Microsoft Ireland *e* Google Pennsylvania *– 7. Alcune osservazioni sul* Cloud Act *– 8. L'accesso ai dati conservati sul* cloud*: la proposta di Regolamento* e-Evidence *– 9. Riflessioni conclusive*

1. Introduzione

Nel giro di poco più di dieci anni, il *cloud computing* ha conosciuto uno sviluppo esponenziale che non accenna a rallentare[1]. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione sinergica di fattori tecnologici (la sovrabbondanza di risorse non utilizzate, lo sviluppo della virtualizzazione, ecc.), nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha imposto nuovi modelli di fruizione dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, resi possibili dalle risorse computazionali, applicative e di *storage* messe a disposizione dagli operatori di *cloud computing*.

Questo sviluppo travolgente si è tuttavia accompagnato a crescenti difficoltà nel trovare un punto di equilibrio tra esigenze diverse e spesso contrapposte, che vanno dalle preoccupazioni per la privacy e la si-

V. Boncinelli è dottore di ricerca in "Teoria del diritto e della politica" presso l'Università degli Studi di Macerata (2005) e svolge la propria attività di consulente informatico specializzato in soluzioni *cloud* e architetture distribuite. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

curezza informatica, alla lotta all'evasione fiscale, dal perseguimento dei reati allo spionaggio industriale. Molto spesso si è finito per concentrarsi su un unico aspetto, trascurando le concrete modalità di funzionamento del *cloud computing* e, più in generale, della rete Internet. Si è così assistito alla proliferazione di obblighi più o meno generalizzati di localizzazione dei dati (*data residency*). Queste misure di localizzazione, per quanto possano assumere le forme più variegate e rispondere ai fini più disparati, sono accomunate dal fatto di porre intenzionalmente ostacoli al flusso di dati attraverso i confini nazionali, ad esempio imponendo di conservare i dati all'interno di server ubicati nel territorio dello Stato, ovvero subordinando il trasferimento dei dati al previo consenso dell'interessato. Il numero di Paesi che hanno introdotto obblighi di questo tipo è in continuo aumento[2]. Uno degli ultimi esempi di questo tipo è rappresentato dall'art. 6, co. 5, del D.L. 30 aprile 2020, n. 28, che nel dettare le linee guida per lo sviluppo della nota piattaforma per la prevenzione e il tracciamento dei casi di Covid-19 ("Immuni"), ha previsto che debba essere "realizzata con infrastrutture localizzate sul territorio nazionale"[3].

Quali che siano le motivazioni dietro all'introduzione di tali misure, è indubbio che stiamo assistendo a un'inversione di tendenza nell'atteggiamento nei confronti dei flussi di dati: se in passato la preoccupazione principale di molti Paesi era quella di mantenere alcune informazioni "al di fuori" dei confini nazionali (si pensi ai sistemi di censura e alla protezione della proprietà intellettuale), oggi gli sforzi maggiori sembrano esser rivolti nel senso opposto, ovvero quello di tenere le informazioni relative ai propri cittadini all'"interno"[4].

Contemporaneamente, però, si assiste anche al fenomeno inverso: quando si tratta di garantire l'interesse pubblico all'accertamento dei reati e all'acquisizione delle prove digitali che si trovano conservate al di fuori del territorio nazionale, anziché guardare al luogo di conservazione dei dati (che costringerebbe le autorità nazionali ad avviare le complesse procedure previste dai trattati di mutua assistenza giudiziaria) si preferisce agire sui soggetti, *in primis* i fornitori di servizi *cloud*, che su tali dati esercitano una qualche forma di controllo, affinché producano le informazioni richieste. In questa direzione si muovono, solo per fare alcuni esempi, tanto il contestatissimo *Cloud Act* del 2018, quanto la proposta di regolamento della Commissione europea relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*), entrambi trattati nelle pagine che seguono.

Si crea così un perverso circolo vizioso, nel quale il proliferare degli obblighi di localizzazione viene assunto come giustificazione delle norme che mirano a "estendere" la giurisdizione degli Stati nazionali al di fuori del loro territorio, con ciò alimentando timori e diffidenze che si traducono nell'adozione di nuovi e più penetranti obblighi di localizzazione. Il problema è che, come accade ogniqualvolta si tenti di regolare in modo settoriale e locale un fenomeno di portata globale, si rischia non solo di non raggiungere il risultato sperato ma, anzi, di moltiplicare e amplificare gli effetti negativi sui diritti dei singoli, sulla sicurezza informatica e la privacy, la libertà di concorrenza e gli investimenti[5].

Scopo di questo contributo non è quello di fornire un'esaustiva ricognizione dei tanti, tantissimi punti critici che si accompagnano ai recenti tentativi di regolazione del fenomeno, né tantomeno di proporre soluzioni generali buone per tutte le stagioni. L'obiettivo, assai più limitato e circoscritto, è quello di evidenziare come, al di là delle definizioni astratte, quando si parla di *cloud computing* si fa in realtà riferimento a un complesso e variegato "ecosistema" di servizi, applicazioni, metodologie e pratiche che presentano tante differenze e peculiarità quanto sono i caratteri in comune. Il problema, ovviamente, non è solo di natura "tassonomica", poiché alla base di qualsiasi tentativo di regolazione del *cloud*, come del resto dell'intera Internet, vi dovrebbe essere la consapevolezza che gli interessi in gioco sono inevitabilmente confliggenti. Ragione in più per evitare tanto un approccio di tipo *one size fits all*, quanto la sua eccessiva "parcellizzazione" in tante legislazioni nazionali e di settore.

2. Un *cloud*, mille *cloud*. Genesi, evoluzione e caratteristiche del *cloud computing*

La storia del *cloud* è disseminata di piccole e grandi innovazioni, la più importante delle quali è stata certamente la nascita e l'inarrestabile diffusione di Internet, che oggi conta 4.5 miliardi di utilizzatori attivi, pari al 59% della popolazione mondiale[6]. Nel ricostruire la genesi del *cloud computing* si è soliti partire dalla tecnologia del *mainframe computing* sviluppata a partire dalla fine degli anni '50 del secolo scorso[7]. Questi costosissimi e ingombranti elaboratori venivano utilizzati per processare dati ed effettuare calcoli che oggi potrebbero essere svolti senza fatica anche dal più economico *smartphone* disponibile sul mercato. Se confrontati con gli standard odierni, questi sistemi erano estremamente difficili

da usare, privi com'erano di un'interfaccia umana, o persino di una tastiera, e programmati mediante schede perforate o nastri magnetici.

Considerato che un'università o un'azienda normalmente potevano permettersi al massimo uno o due *mainframe*, era necessario ottimizzare al massimo l'utilizzo delle risorse computazionali. L'idea alla base della condivisione delle risorse nasceva da una semplice constatazione: l'inserimento di un programma all'interno dell'elaboratore richiedeva un tempo considerevole, durante il quale le capacità computazionali rimanevano in larga parte inutilizzate. Al contrario, un ampio gruppo di utenti che lavoravano contemporaneamente avrebbe permesso di utilizzare le pause di un utente intento a inserire dati per destinare il tempo di elaborazione a vantaggio degli altri. Di qui l'elaborazione di metodi di *time-sharing* in grado di consentire a più utenti di condividere le risorse del *mainframe*, utilizzando dei terminali privi di una propria capacità di elaborazione (e per questo definiti anche *dumb terminal* o, con un'espressione tornata recentemente alla ribalta proprio in connessione con lo sviluppo del *cloud computing*, *thin client*).

Un'altra importante innovazione fu rappresentata dalla "virtualizzazione". A cavallo degli anni '60 e '70 furono rilasciati i primi sistemi operativi in grado di supportare la possibilità di condividere un insieme di risorse hardware (dischi rigidi, processori, ecc.) tra più sistemi operativi "virtuali" che "convivono" sullo stesso computer fisico. Questi sistemi operativi virtuali sono completamente isolati gli uni dagli altri, e possono utilizzare soltanto le risorse di tipo "logico" (capacità computazionale, di *storage*, di connettività, ecc.) messe a disposizione dal sistema di virtualizzazione, e da questo dinamicamente allocate tra le varie macchine virtuali a seconda delle esigenze (*pooling*).

Sebbene i concetti fondamentali del *cloud computing* risalgano dunque agli albori dell'informatica, l'uso del termine *cloud* per indicare un nuovo modo di accedere al software, potenza di calcolo e capacità di archiviazione dei dati attraverso il web è invece relativamente recente. Contrariamente a quanto si potrebbe pensare, l'espressione *cloud computing* non è nata nell'ambiente *hi-tech*, ma è stata coniata durante una (si presume fumosa) riunione dei responsabili del *marketing* tenutasi nel 1996 negli uffici di Houston della Compaq Computer. L'espressione non indicava tanto un insieme specifico di tecnologie, quanto piuttosto un diverso modello di consumo dei servizi informatici tramite Internet[8].

Le origini del termine spiegano forse il perché il concetto di *cloud*, con i suoi contorni indefiniti ed evanescenti, abbia sin da subito creato difficoltà, equivoci e incomprensioni (che continuano a tutt'oggi) non solo tra gli addetti ai lavori, ma anche per i governi che a più riprese sono intervenuti nel tentativo di regolare il fenomeno, i quali si sono trovati nella necessità di definire cosa rientri nel concetto di *cloud computing* e cosa no. Non a caso, una delle prime pubblicazioni dedicata al *cloud computing* da parte del *National Institute for Standards and Technology* (NIST), a cui si deve peraltro la più citata definizione di *cloud*, si apre con l'affermazione per cui «Cloud computing can and does mean different things to different people»[9]. In altre parole, non esiste un solo *cloud*. Come vedremo nelle prossime pagine, una parte consistente dei problemi che nascono sul piano della regolazione del fenomeno possono essere affrontati solo se si tengono in debito conto le peculiarità dei diversi modelli di *cloud*.

Dunque, di *cloud computing* esistono svariate definizioni, che pongono l'accento ora su alcuni caratteri, ora su altri[10]. Tuttavia, un aspetto generale su cui le varie formulazioni convergono è l'idea per cui il *cloud* abbia rappresentato un completo mutamento di paradigma rispetto alle forme tradizionali di utilizzo dei servizi informatici[11].

Volendo partire da una definizione comunemente accettata, possiamo prendere a prestito quella offerta proprio dal NIST: «Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction»[12].

Proviamo a specificare meglio la definizione sopra riportata, evidenziando alcune caratteristiche essenziali. Per prima cosa, il *cloud* introduce (o consiste di) una serie di livelli di "astrazione" che permettono di utilizzare determinate risorse senza doversi preoccupare della loro gestione, configurazione, manutenzione, messa in sicurezza, ecc. Sebbene la ripartizione delle responsabilità tra fornitore del servizio e utilizzatore vari in base al "modello di servizio" (su cui torneremo più avanti), l'elemento comune è che le risorse utilizzate dall'utente hanno, come si è accennato parlando di virtualizzazione, un carattere prettamente logico, anziché "fisico".

Tali risorse sono messe in comune per servire molteplici utenti mediante un modello condiviso (c.d. *multi-tenant*), assegnate e riassegnate dinamicamente in base alla domanda (*resource pooling*). Possono essere accedute, create, gestite o dismesse direttamente dall'utente, con poca o nessuna interazione con il fornitore e tramite meccanismi stan-

dard, accessibili via Internet da piattaforme eterogenee (*broad network access*), e utilizzate in piena autonomia, secondo le proprie necessità (*on-demand self-service*). Le risorse possono essere inoltre acquisite e rilasciate in modo elastico, in alcuni casi anche automaticamente, per scalare[13] rapidamente le capacità del sistema in relazione alla domanda (*rapid elasticity*). Infine, i sistemi *cloud* monitorano e ottimizzano costantemente l'uso delle risorse (*measured service*), facendo leva sulla capacità di misurazione ad un livello di astrazione appropriato per il tipo di servizio (ad esempio memoria, elaborazione, larghezza di banda e utenti attivi) e, in genere, con costi legati all'utilizzo delle risorse[14].

3. I principali modelli di servizio

Sulla base della definizione sopra riportata, il NIST individua tre specifici "modelli di servizio", distinti in base al tipo di risorsa messa a disposizione e al ruolo riservato all'utente che acquista il servizio: si parla così di *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS), e *Software-as-a-Service* (SaaS).

In un servizio di tipo IaaS, il fornitore del servizio *cloud* mette a disposizione i componenti necessari a realizzare una propria infrastruttura informatica virtuale. Rispetto a una tradizionale infrastruttura locale, costituita da server, dischi rigidi e sistemi di rete che devono essere acquistati o noleggiati, gestiti per tutto il loro ciclo di vita e sostituiti in caso di problemi, un'infrastruttura *cloud* si basa sul carattere puramente "virtuale" delle risorse. Questo significa, tra le altre cose, che gli utenti non devono preoccuparsi dell'installazione, della configurazione e della manutenzione dell'hardware e dei sistemi infrastrutturali, che è a totale carico del fornitore *cloud*. Gli utenti rimangono invece responsabili della configurazione dei sistemi che vengono eseguiti sull'infrastruttura virtuale (come i sistemi operativi e le applicazioni che ci girano sopra). I più diffusi servizi IaaS sono rappresentati da macchine virtuali, servizi di *storage* dei dati e servizi di rete virtuali (*virtual networking*).

In un servizio di tipo PaaS, invece, la piattaforma mette a disposizione dell'utente l'ambiente di esecuzione di un'applicazione (quale ad esempio un sito web), a mantenerlo in esecuzione anche in caso di problemi nei livelli sottostanti dell'infrastruttura (grazie a sofisticati meccanismi di *fault-tolerance* e di replica geografica dei dati), garantendo inoltre alti livelli di performance e di scalabilità del servizio. In un servizio PaaS, il fruitore non si deve preoccupare dell'infrastruttura, della connettività, della configurazione del sistema operativo o di altri aspetti legati all'ambiente di esecuzione. Tutti questi dettagli sono a carico del fornitore *cloud* e all'utente resta la sola responsabilità di gestire l'applicazione[15].

Infine, le soluzioni SaaS liberano gli utenti sia dalla gestione del sistema operativo, che dalla supervisione dell'applicazione: tutto ricade nelle mani del fornitore del servizio. Tutto quello che l'utente deve fare è usare l'applicazione messa a disposizione dal fornitore senza doversi preoccupare di altro. Tipicamente, i servizi SaaS sono usufruiti tramite un *web browser*, e tanto i dati applicativi quanto il carico di lavoro sono trasferiti sull'infrastruttura dell'operatore *cloud*, il che rende possibile sfruttare un'ampia gamma di funzionalità direttamente dallo schermo del proprio *smartphone* o da qualunque altro dispositivo connesso a Internet. A essere interessati da questa trasformazione non sono soltanto gli utenti finali, ma anche le aziende e le pubbliche amministrazioni. Gran parte del lavoro che prima veniva svolto sfruttando applicazioni e servizi installati in locale (sui server aziendali o direttamente sulle postazioni lavorative), si avvale oggi del web per numerose funzioni (dall'archiviazione dei dati alle analisi di *business intelligence*, dai filtri *antispam* alla lotta al *malware*).

Con il tempo, accanto a questi tre modelli tradizionali se ne sono aggiunti di nuovi. Nel tentativo di dare specifico risalto alle peculiarità dei nuovi servizi lanciati a un ritmo quasi giornaliero, e forse anche per venderli meglio, sono stati elaborati un gran numero di acronimi (es. *Database-as-a-Service*, *Storage-as-a-Service*, *Disaster Recovery-as-a-Service*, *Workplace-as-a-Service*, *Desktop-as-a-service*, ecc.)[16]. Di recente, vista l'impossibilità di arginarne la proliferazione, è stata proposta anche un'ulteriore tipologia, definita "XaaS" (o *X-as-a-Service*), dove la "X" sta a indicare non tanto uno specifico modello di servizio, quanto piuttosto una sorta di categoria residuale entro cui ricondurre tutti quei servizi *cloud* che non si lasciano facilmente incasellare in una delle tre categorie tradizionali, vuoi perché se ne differenziano sotto aspetti rilevanti, vuoi perché presentano elementi di tutte e tre le classificazioni precedenti.

Questo tipo di classificazione ha ovviamente un valore puramente esemplificativo e non ha alcuna pretesa di esaustività delle differenze e delle particolarità dei numerosi servizi *cloud* oggi disponibili sul mercato. Quando, poco più di dieci anni fa, questa classificazione si è affermata tra gli addetti ai lavori, i servizi offerti erano relativamente pochi (macchine virtuali, servizi di rete, applicazioni web, ecc.). In quel contesto, la distinzione tra IaaS, PaaS e SaaS era sufficiente a descrivere, se non tutti, la gran par-

te dei servizi offerti. Negli ultimi anni si è assistito al proliferare di decine e decine di nuovi servizi, sempre più sofisticati ed evoluti. Oggi si contano centinaia di servizi *cloud* diversi, che sono andati ad arricchire l'offerta accanto a quelli più "tradizionali": servizi di intelligenza artificiale e *machine learning*, analisi dei dati, *Internet of Things* (IoT), *blockchain* e cripto-valute, *streaming* di contenuti multimediali, realtà aumentata (*augmented reality*), sicurezza informatica, servizi per dispositivi mobili, ecc.

Anche con tutti questi limiti, tuttavia, la distinzione tra IaaS, PaaS e SaaS ha una sua rilevanza. Come abbiamo visto, nel caso di servizi IaaS e PaaS l'utente ha un controllo molto più accentuato sui dati, potendo innanzitutto scegliere dove tali dati devono essere conservati, partizionati o replicati. Nel caso di servizi SaaS, invece, l'utente non ha in genere alcun controllo su dove i dati sono conservati o sulle misure di sicurezza applicate. Tra queste ultime, una menzione particolare va alla cifratura dei dati conservati o in transito sull'infrastruttura. Nei servizi SaaS, la scelta di cifrare o meno i dati di cui è "titolare" l'utente del servizio (ad esempio le fatture dei clienti, le e-mail, i messaggi scambiati in software, i dati di produzione, ecc.) ricade sul fornitore del servizio software, che decide anche le modalità di gestione delle relative chiavi. Nei servizi di tipo IaaS e PaaS, la gestione di questi aspetti è lasciata per lo più all'utente, e dipende in buona sostanza dal livello di sicurezza che quest'ultimo mira a implementare[17]. Queste differenze nel grado di libertà lasciato all'utilizzatore del servizio discendono dal fatto che, mentre questi ultimi due modelli sono rivolti principalmente a organizzazioni, pubbliche o private, dotate delle necessarie competenze tecnologiche e professionali, i servizi SaaS, nella misura in cui sollevano l'utente da qualunque responsabilità in merito alla loro gestione, possono essere utilizzati da chiunque, sia esso un utente finale o un'organizzazione (si potrebbe dire, sotto questo profilo, che sono servizi "chiavi in mano").

In altri termini, i servizi infrastrutturali (così come la maggior parte di quelli PaaS, in cui la "piattaforma" può essere vista come una sorta di "ponte" tra l'infrastruttura e il servizio applicativo finale), oltre a rappresentare un modello alternativo alla gestione in proprio di risorse informatiche (con tutti i benefici che ne derivano in termini di risparmio e flessibilità), possono essere visti anche come una "borsa degli attrezzi" a cui attingere per "confezionare" servizi applicativi ad alto valore aggiunto (come ad esempio sistemi per la gestione e la fidelizzazione dei clienti, per la pianificazione delle risorse aziendali, ovvero per facilitare lo *smart-working* e la collaborazione da remoto, ecc.) destinati ad essere rivenduti a clienti finali (altre organizzazioni o persone fisiche).

Questo rilievo mette in luce un aspetto spesso sottovalutato quando si tratta di elaborare le regole da applicare al *cloud computing*. Sempre più spesso, infatti, la realizzazione di una soluzione *cloud* comporta la combinazione di molteplici servizi, di natura anche assai diversa e con l'intervento di fornitori terzi. Tale complessità è in genere "trasparente"[18] dal punto di vista dell'utente finale, il quale si limita a utilizzare il servizio senza rendersi conto della sottostante complessità. Ad esempio, se dalla prospettiva di un utente, il servizio di archiviazione *cloud* di Dropbox può apparire come un classico SaaS, dietro le quinte il servizio ha utilizzato per molti anni l'infrastruttura messa a disposizione da un altro fornitore (in questo caso Amazon AWS)[19]. Dropbox era dunque al tempo stesso un utilizzatore di servizi di tipo IaaS (forniti da Amazon) e, dal punto di vista dei suoi utenti, un fornitore di servizi di tipo SaaS.

La struttura naturalmente aperta e "partecipativa" del *cloud* pone non pochi interrogativi quando si tratta, ad esempio, di definire formalmente i ruoli dei vari soggetti coinvolti nel trattamento di dati personali. Come vedremo meglio nelle prossime pagine, tutte queste differenze giocano un ruolo importante anche sul piano degli effetti della regolazione. Lo stesso vale, seppur sotto altri profili, per i diversi modelli di distribuzione dei servizi *cloud* oggi presenti sul mercato, che si distinguono principalmente in base ai loro destinatari.

4. I modelli di distribuzione del *cloud computing*

Accanto ai tre modelli di servizio, il NIST individua infatti anche quattro modelli di distribuzione, distinguendo tra *cloud* pubblici, privati, "comunitari" (*community cloud*) e ibridi.

In un *cloud* pubblico, la modalità di distribuzione di gran lunga più comune e diffusa, l'infrastruttura è predisposta per essere utilizzata dalla generalità degli utenti. Le risorse sono di proprietà del fornitore e vengono distribuite tramite Internet a chiunque ne faccia richiesta (esempi di *cloud* pubblici sono Amazon Web Services, Microsoft Azure e Google Cloud). Nel *cloud* pubblico le risorse hardware sono condivise dai vari utenti (o *tenant*) e allocate secondo logiche che ne massimizzano l'efficienza.

In un *cloud* privato, invece, l'infrastruttura tecnologica è predisposta per essere utilizzata in via esclusiva da una singola organizzazione. In questo caso, a consumare le risorse condivise sono in genere le diverse unità che compongono l'organizzazione

(dipartimenti, direzioni, uffici, ecc.). Tanto l'ubicazione fisica quanto la proprietà dell'infrastruttura è irrilevante: può essere gestita direttamente dall'organizzazione o affidata, in tutto o in parte, a fornitori terzi, così come può comprendere un solo *data center* situato all'interno dei locali dell'organizzazione, ovvero più *data center* distribuiti in località diverse. Quello che conta è che nell'infrastruttura, anche se gestita da un terzo, tutte le risorse sono dedicate a uno specifico cliente. Molto spesso le organizzazioni di una certa dimensione optano per un *cloud* privato (magari riconvertendo l'infrastruttura tradizionale già esistente) per motivi legati alla sicurezza dei dati (dal momento che questi rimangono all'interno del perimetro dell'organizzazione), ovvero per soddisfare particolari requisiti di localizzazione previsti da normative di settore, o ancora per il tipo particolare di applicazioni utilizzate dall'azienda.

Il *cloud* comunitario, nonostante il nome, è assimilabile *in toto* a quello privato, con la sola differenza che in questo caso l'infrastruttura è messa a esclusiva disposizione di più organizzazioni che hanno obiettivi o necessità (es. di sicurezza, normativi, ecc.) condivise. Come un qualsiasi *cloud* privato, può essere gestito da una o più organizzazioni della comunità o affidato, in tutto o in parte, a un fornitore terzo (che può consistere, ad esempio, in un raggruppamento temporaneo di imprese).

Nel *cloud* ibrido, infine, *cloud* pubblici e privati sono integrati per svolgere funzioni distinte all'interno della stessa organizzazione. Negli ultimi anni questa forma di *cloud* ha conosciuto una notevole diffusione, acquisendo sempre maggiori quote di mercato rispetto agli altri modelli di distribuzione[20], grazie ai vantaggi che presenta per le organizzazioni, che possono sia usufruire delle risorse illimitate (e poco costose) messe a disposizione dal *cloud* pubblico, sia soddisfare particolari esigenze di sicurezza o di *compliance* normativa garantite dal *cloud* privato.

Ciascun modello di distribuzione porta con sé vantaggi e svantaggi. In generale, tanto i *cloud* pubblici che quelli privati sono caratterizzati da un'alta efficienza grazie alla virtualizzazione e alla condivisione delle risorse, consentendo così un migliore bilanciamento del carico di lavoro; da un'elevata disponibilità, che minimizza i tempi di inattività e migliora la continuità aziendale; nonché da una scalabilità elastica (che nel caso di *cloud* privati incontra tuttavia un limite nelle risorse fisiche non infinite a disposizione di un'organizzazione, mentre in quello pubblico sono virtualmente illimitate).

Alcuni vantaggi, invece, sono specifici del *cloud* pubblico, quali bassi costi iniziali (mentre in quello privato sono particolarmente elevati); elevate economie di scala in termini di potere di acquisto delle apparecchiature che di efficienza nella gestione; semplicità di gestione, in quanto l'infrastruttura è gestita, configurata e mantenuta dal fornitore (mentre in quello privato sono richieste competenze tecniche specifiche, oltre che capacità organizzative e disponibilità economiche al di fuori della portata di molte organizzazioni).

Di contro, il *cloud* privato consente, come si è detto, di avere un maggiore controllo in tema di sicurezza e conformità normativa, nonché di garantire una maggiore qualità del servizio, poiché l'infrastruttura può essere configurata e ottimizzata per venire incontro alle specifiche esigenze di un'organizzazione[21].

Sulla base di questa classificazione, un'eventuale infrastruttura *cloud* gestita da o per conto di soggetti che svolgono compiti e funzioni di natura pubblica si configurerebbe comunque come *cloud* privato (o comunitario, qualora condiviso da più soggetti), indipendentemente dal fatto che a fornire (e a gestire) l'infrastruttura sia o meno un soggetto pubblico. L'unico elemento rilevante, in questo schema, è infatti il carattere esclusivo delle risorse *cloud* usufruibili, e non la "natura" del soggetto (o dei soggetti) che, a seconda dei casi, forniscono o utilizzano detti servizi[22].

5. Una classificazione alternativa di *cloud computing*: *Data Shard*, *Data Localization*, *Data Trust*

Le tradizionali classificazioni dei servizi *cloud* sin qui sommariamente illustrate dovrebbero aver già lasciato intuire la complessità dei modelli che stanno dietro l'erogazione di servizi apparentemente semplici, se considerati dal punto di vista dell'utente finale. A queste classificazioni, però, se ne affianca un'altra che riveste un'importanza assolutamente centrale quando si affrontano le tematiche relative alla localizzazione dei dati, perché basata sulla diversa modalità di gestione dell'infrastruttura, o meglio dei dati che su tale infrastruttura circolano: *Data Shard*, *Data Localization* e *Data Trust*[23].

Nel modello definito *Data Shard*, l'informazione è divisa, o meglio "partizionata", in molteplici "frammenti" (*shard*) dispersi in vari nodi della rete. Tramite il partizionamento, un archivio di grandi dimensioni viene suddiviso in "componenti" più piccoli, più efficienti e "maneggevoli" rispetto all'originale[24]. Alle strategie di partizionamento si ricorre in genere per migliorare le performance delle operazioni che coinvolgono grandi volumi di dati, ovvero per "avvicina-

re" i dati agli utenti sulla base della loro ubicazione geografica, in modo da ridurre i tempi di latenza e migliorare le prestazioni complessive[25]. Le ragioni che stanno dietro questo tipo di strategie sono dunque di natura eminentemente tecnica: «The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world»[26].

Nel modello denominato *Data Localization*, il fornitore dei servizi *cloud* conserva i dati all'interno di un certo ambito geografico che, a seconda dei casi, può avere estensioni assai diverse, e che solo occasionalmente coincide con i confini di uno Stato. Nell'individuazione dei diversi ambiti geografici in cui suddividere l'infrastruttura concorrono molteplici ragioni, di natura economica, tecnica e, non ultima, legale, come l'esistenza di obblighi positivi di localizzazione dei dati (es. Francia e Germania).

Solitamente, l'infrastruttura globale dei grandi operatori di servizi *cloud* comprende più aree geografiche o regioni più o meno estese (ad esempio Europa centrale, Stati Uniti occidentali, ecc.). Ciascuna di queste aree è, a livello infrastrutturale, completamente autonoma e indipendente dalle altre, così da garantire la massima stabilità e tolleranza ai guasti. Ogni area o regione è a sua volta suddivisa in più zone di disponibilità. Queste zone, che comprendono uno o più *data center* muniti di impianti indipendenti per l'energia, il raffreddamento e la rete, sono fisicamente isolate le une dalle altre, ma connesse tramite collegamenti dedicati a bassa latenza. Mediante la suddivisione di un'area in zone più circoscritte si cerca di garantire la costante disponibilità dei servizi all'interno di quell'area, mediante la replica delle risorse in diverse zone geografiche, di modo che queste siano sempre accessibili anche quando, ad esempio a seguito di una calamità naturale, si verificano dei problemi in uno o più *data center*[27].

Il modello di *Data Trust* è senz'altro quello più interessante ai fini della nostra discussione, se non altro perché non nasce per soddisfare esigenze tecniche, quanto piuttosto come tentativo, da parte dei fornitori di servizi *cloud* (in questo caso Microsoft), di trovare una via d'uscita da una situazione sempre più insostenibile. Come vedremo meglio nelle prossime pagine, infatti, l'approvazione del *Cloud Act* da parte del Congresso USA e la conseguente pretesa di poter accedere ai dati degli utenti custoditi dai fornitori *cloud* americani indipendentemente dal luogo in cui sono conservati, ha gettato ulteriore benzina sui timori di indesiderate interferenze da parte degli Stati Uniti sui dati dei cittadini di altri Paesi[28]. Di fronte al moltiplicarsi degli obblighi di localizzazione dei dati, spaventati dalla possibilità di perdere rilevanti quote di mercato a favore di concorrenti più piccoli, ma fuori dalla portata del governo americano, alcune aziende d'oltreoceano hanno finito per elaborare un approccio assolutamente originale, che combina elementi legali, organizzativi e tecnici per separare nettamente la gestione dell'infrastruttura dall'accesso ai dati che su tale infrastruttura insistono.

Nel modello di *Data Trust*, elaborato a partire da concetti e istituti giuridici di origine anglosassone, il fornitore di servizi *cloud* si avvale infatti di un soggetto esterno, detto *data trustee*, per la gestione di tutto ciò che esula dalla stretta manutenzione operativa dell'infrastruttura. L'elemento giuridico essenziale è dato dal ricorso alla figura negoziale del *trust*[29], mediante il quale il fornitore si spoglia completamente della facoltà giuridica di accedere ai dati che transitano sull'infrastruttura per affidarli a una terza parte (nel caso in questione, una sussidiaria della tedesca Deutsche Telekom). Qualsiasi attività operativa svolta dal fornitore dell'infrastruttura che potrebbe potenzialmente consentire l'accesso ai dati dei clienti (come ad esempio la gestione degli incidenti, l'aggiornamento del software, ecc.) è soggetta a controlli tecnici che richiedono l'approvazione e la supervisione esplicite del fiduciario dei dati. L'accesso ai sistemi è inoltre consentito solo nell'ambito di un servizio specifico, per uno scopo definito, e solo per il tempo strettamente necessario allo svolgimento delle attività tecniche, che sono strettamente registrate e monitorate.

Sul piano tecnico, la separazione dei profili relativi alla gestione dell'infrastruttura da quelli dell'accesso ai dati viene garantita, oltre che dalla segregazione fisica e logica di reti e sistemi, principalmente da meccanismi di cifratura dei dati, le cui chiavi sono conservate in via esclusiva dal fiduciario. Tutte le richieste di accesso ai dati, dunque, devono essere indirizzate al *trustee* (l'unico in possesso delle chiavi di cifratura), il quale sarà tenuto a valutarle esclusivamente sulla base del diritto nazionale. Proprio l'elaborazione del principio di separazione tra la gestione dell'infrastruttura e l'accesso ai dati che su di essa insistono rappresenta uno degli elementi maggiormente innovativi e, possibilmente, più dirompenti dell'attuale panorama dei servizi di *cloud computing*.

È opportuno precisare, prima di continuare oltre, che questi diversi modelli non si escludono necessariamente l'un l'altro, ma – entro certi limiti – possono combinarsi variamente all'interno di una stessa soluzione. Il modello di *Data Trust* tedesco, ad esempio, prevede che i dati siano conservati all'interno dei confini nazionali (*Data Localization*), anche se – dal punto di vista teorico – questo non sembra essere

un requisito necessario per raggiungere le finalità che tale modello persegue (prima fra tutte quella di evitare l'insorgere di conflitti di giurisdizione), poiché le modalità tecniche, organizzative e legali adottate sono di per sé sufficienti a escludere qualunque accesso esterno ai dati stessi (anche qualora, in ipotesi, fossero localizzati in *data center* collocati in altri Paesi europei). Né l'eventuale presenza di obblighi di localizzazione esclude, di per sé, il ricorso alle tecniche di partizionamento dei dati (*Data Shard*), anche se queste avranno una portata assai più limitata, potendo riguardare unicamente *data center* collocati entro i confini nazionali (con ciò sacrificando in misura significativa l'efficacia complessiva del sistema).

Nei prossimi paragrafi ci soffermeremo su alcuni dei passaggi salienti che hanno caratterizzato l'accidentato percorso seguito dalla giurisprudenza e dal legislatore USA in tema di accesso ai dati custoditi su *cloud* da parte delle pubbliche autorità. In questo breve *excursus* non si può non partire dalla celebre decisione della corte d'appello nel caso *Microsoft Ireland*, che, dando prevalenza all'ubicazione geografica dei dati, ha riconosciuto il diritto del fornitore a non ottemperare all'ordine delle autorità federali di comunicare il contenuto di e-mail conservate nel territorio irlandese. Vedremo anche come tale decisione, al netto delle questioni ermeneutiche di diritto interno, sia stata di fatto resa possibile dal particolare modello di servizio utilizzato dall'operatore *cloud* (di tipo *Data Localization*). Vedremo anche come siano state sempre le effettive modalità di gestione del servizio *cloud* a rendere impossibile l'applicazione dello stesso principio in un caso apparentemente identico (*Google Pennsylvania*), perché espressione di un diverso modello di *cloud* (*Data Shard*). Infine, accenneremo agli aspetti salienti del *Cloud Act*, approvato dal Congresso USA proprio per disinnescare le potenziali conseguenze della decisione del caso *Microsoft Ireland*, ma che ha finito per ottenere il risultato opposto rispetto a quello perseguito, a dimostrazione di come la complessità e la varietà dei modelli *cloud* siano state, ancora una volta, sostanzialmente ignorate.

6. L'approccio al *cloud* al di là dell'oceano: i casi *Microsoft Ireland* e *Google Pennsylvania*

Il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* è stato adottato dal Congresso USA nel marzo del 2018 come risposta alla decisione della corte d'appello nel caso *United States v. Microsoft Corp.*[30]. In quell'occasione, Microsoft si era opposta a un ordine (*warrant*) emesso dalle autorità federali americane sulla base delle disposizioni dello *Stored Communication Act* (SCA) del 1986, di produrre, tra le altre cose, il contenuto di e-mail riconducibili a un determinato *account* di posta elettronica[31].

Microsoft, che pure aveva fornito alle autorità i dati custoditi sui server in territorio americano, si era rifiutata di dare accesso ai contenuti delle e-mail perché conservate nei suoi *data center* di Dublino, dunque al di fuori del territorio statunitense, con ciò suggerendo l'idea della prevalenza dell'ubicazione "fisica" dei dati nella determinazione della giurisdizione. Nell'accogliere il ricorso di Microsoft e ribaltare la decisione di primo grado, il giudice d'appello muove infatti dal rilievo secondo cui Microsoft archivia i dati associati al contenuto della posta elettronica dei propri utenti su oltre cento *data center* sparsi per il mondo. Quando viene creato un *account*, l'utente seleziona automaticamente un "codice Paese" e Microsoft archivia il contenuto delle e-mail associate a quell'*account* (nonché tutta una serie di contenuti ulteriori, quali documenti, calendari, ecc.) nel *data center* più vicino al Paese identificato dall'utente[32]. L'ubicazione fisica dei dati è, per la corte, l'elemento oggettivo da cui partire per decidere dell'applicabilità extra-territoriale delle disposizioni dello SCA: «Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States»[33].

Quando, nel 1986, il Congresso approvò lo SCA come parte del più ampio *Electronic Communications Privacy Act*, l'obiettivo era quello di proteggere la privacy degli utenti nel contesto dei nuovi mezzi tecnologici che richiedono l'interazione di un utente con un fornitore di servizi, anche perché "trent'anni fa, i confini internazionali non venivano attraversati così regolarmente come lo sono oggi", grazie a reti e infrastrutture hardware sparse in tutto il mondo per soddisfare le richieste degli utenti. Né esplicitamente, né implicitamente, lo SCA prende in considerazione l'applicazione delle sue disposizioni al di fuori del territorio americano. E questa – conclude la corte – è esattamente la vera questione del giudizio: «It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. (...) It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and

policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our border»[34].

La decisione ha sorpreso molti commentatori perché, nell'offrire una lettura molto più restrittiva delle norme dello SCA (e in particolare dell'istituto del *warrant*), ha messo in discussione il tradizionale test in base al quale l'elemento critico nel determinare se l'ordine di produrre la documentazione richiesta sia o meno eseguibile è dato dal fatto che il destinatario abbia o meno "il controllo, la custodia o il possesso" della stessa, indipendentemente dal luogo in cui tali informazioni sono conservate al momento della richiesta[35]. Il timore che la decisione del caso *Microsoft Ireland* potesse porre, ove confermata dalla Corte Suprema davanti alla quale la questione era stata sollevata, un ostacolo alle indagini aventi ad oggetto dati collocati al di fuori del territorio statunitense ha spinto il Congresso ad approvare rapidamente il *Cloud Act*.

Il carattere "eccezionale" del caso *Microsoft Ireland* è stato spesso ricondotto alla diversa lettura offerta dalla corte d'appello circa l'estensione dello SCA al di fuori del territorio americano. A riprova di tale carattere viene solitamente citato il caso *Google Pennsylvania*, di poco successivo al primo, nel quale il giudice ribalta il principio espresso nel caso Microsoft e impone al fornitore *cloud* di ottemperare all'ordine emesso dalle autorità federali[36]. Solo pochi commentatori hanno invece evidenziato come l'opposto risultato raggiunto nei due casi dipenda in larga parte dal diverso modello di *cloud* al centro della contesa[37].

Nel caso *Google Pennsylvania*[38], infatti, a essere coinvolti erano una serie di servizi i cui dati sono suddivisi in componenti che la sottostante infrastruttura provvede a smistare tra vari nodi della sua rete globale, spostandoli automaticamente da un nodo all'altro sulla base di logiche di natura prettamente tecniche, legate alla complessiva efficienza e affidabilità del sistema. Si trattava insomma di un caso di *Data Shard*, secondo la classificazione esposta nella prima parte del contributo.

Il caso riguardava due *search warrant* emessi per dati associati ad altrettanti *account* di utenti di Google. Quest'ultimo, da parte sua, aveva parzialmente ottemperato alla richiesta fornendo informazioni archiviate in *data center* situati negli Stati Uniti. Al tempo stesso, basandosi sul precedente Microsoft, si era rifiutata di fornire i dati che, in base a logiche interne di partizionamento, si trovavano su server collocati all'estero. Uno dei passaggi fondamentali seguiti dalla corte nell'arrivare alla conclusione positiva circa l'obbligo di Google di fornire per intero le informazioni richieste muove proprio dalla questione relativa a come i dati siano stati partizionati e dove si trovino i vari *shard*[39]: «Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process. (...) Google's architecture not only divides user data among data centers located in different countries, but also partitions user data into shards. Furthermore, the data automatically moves data from one location on Google's network to another as frequently as needed, to optimize for performance, reliability, and other efficiencies. Because of the structure of this system, Google cannot say with any certainty which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process»[40].

Secondo la Corte, piuttosto che a mere *possibilities and legal abstractions*, occorre guardare alla realtà dei fatti. In questo caso, la realtà era che Google avrebbe potuto accedere a tutte le informazioni direttamente dalla sede centrale in territorio americano, a nulla rilevando l'ubicazione fisica dei dati, che in questo caso è così frammentaria da considerarsi evanescente. Il ricorso al criterio del "possesso, custodia o controllo" è dunque una strada resa necessaria dalla natura stessa del servizio *cloud*. L'opposto orientamento mostrato dalla corte d'appello nel caso Microsoft nasce dalla diversa configurazione del servizio *cloud* al centro della contesa, nel quale tutti i dati rilevanti erano conservati "in via esclusiva e in modo stabile" nel suo *data center* irlandese. Nel caso *Google*, invece, il giudice muove dalla constatazione secondo cui non sussiste alcuna prova circa l'esatta ubicazione dei server su cui sono ospitate le informazioni richieste dalle autorità federali.

«Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a "seizure" because there is no meaningful interference with the account holder's possessory interest in the user data. Indeed, (...) Google regularly transfers user data from one data center to another without the customer's knowledge. Such transfers do not interfere with the customer's

access or possessory interest in the user data. Even if the transfer interferes with the account owner's control over his information, this interference is de minimis and temporary».

Il fatto che l'operatore *cloud* ricorra a tecniche di partizionamento per massimizzare l'efficienza dell'infrastruttura, in modo del tutto invisibile e trasparente per l'utente finale (che anzi non ha alcuna idea circa l'ubicazione dei propri dati, né tantomeno delle sottostanti logiche di partizionamento) implicherebbe, secondo la corte, che non si possa parlare di interferenza con il possesso dei dati da parte dell'utente. Se, per effetto di queste logiche interne, i dati si trovano partizionati in *data center* collocati all'estero, questo rappresenta un elemento del tutto accidentale, perché in fondo neppure il fornitore saprebbe indicare con precisione dove e in quali server sono presenti questi frammenti[41]. L'unico elemento rilevante è, per la Corte, la possibilità di accedere ai dati, nella loro forma "ricomposta", dalla sede centrale del fornitore, situata in territorio USA e come tale soggetta all'osservanza delle norme federali.

Nel confermare l'obbligo di Google di adempiere a quanto richiesto dalle autorità USA, il giudice esclude però che questo comporti un'applicazione extraterritoriale alle disposizioni dello SCA. L'argomento principale sembra essere dunque di natura prettamente contingente, relativo al particolare modello di servizio *cloud* al centro della questione: «No one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified»[42].

Mettendo a confronto il caso *Microsoft Ireland* con il caso *Google Pennsylvania*, è facile notare come le due decisioni abbiano ad oggetto modelli di servizio e di gestione del *cloud* assai diversi[43]. La prevalenza al criterio dell'ubicazione fisica dei dati nel primo, così come la prevalenza del criterio del controllo sui dati, nel secondo, dipendono in ultima analisi dal tipo di servizio al centro della discussione. Nel caso Microsoft, l'applicazione del criterio del luogo di residenza dei dati è resa possibile dal particolare modello di gestione dell'infrastruttura, in cui l'informazione si trova stabilmente ubicata all'interno di confini definiti (*Data Localization*). Questa caratteristica tecnica del servizio, frutto di scelte più o meno arbitrarie dell'operatore *cloud*, rappresenta l'elemento che abilita, sul piano pratico, la discussione sull'eventuale efficacia extraterritoriale delle norme che ne prevedono la confisca o il sequestro, alla pari di qualunque altro oggetto fisico.

Anche nel caso Google sono i caratteri contingenti del servizio a indirizzare e condizionare l'inquadramento legale del caso. Qui, le modalità tecniche scelte dal fornitore per ottimizzare la complessiva infrastruttura (*Data Shard*) rendono virtualmente impossibile ricorrere al criterio della ubicazione dei dati, sia dal punto di vista concettuale che da quello pratico. Questi vengono infatti spostati e riallocati continuamente da un nodo della rete ad un altro sulla base di logiche interne, largamente automatizzate, che rendono difficilmente percorribili i tradizionali canali della cooperazione giudiziaria internazionale. La vera questione, secondo il giudice, non è tanto l'applicabilità extraterritoriale delle disposizioni dello SCA, quanto piuttosto il rischio, concretissimo, di rendere eccessivamente difficoltoso, o addirittura impossibile, l'accesso alle informazioni da parte delle forze di polizia e dell'autorità giudiziaria: il timore del c.d. *going dark*.

7. Alcune osservazioni sul *Cloud Act*

Se è vero che esistono sostanziali differenze tra Stati Uniti e Unione europea in merito agli standard di protezione dei dati personali, che il *Cloud Act* ha peraltro contribuito ad acuire, è anche vero che quest'ultimo si proponeva, almeno nelle intenzioni, di facilitare la cooperazione internazionale attraverso lo strumento degli *executive agreement* e, al tempo stesso, offrire alle aziende destinatarie delle richieste di accesso un meccanismo giuridicamente azionabile per contestarne la legittimità. Alla base della soluzione prescelta dal legislatore USA vi erano infatti alcune condivisibili preoccupazioni. In primo luogo, l'aumento esponenziale delle richieste di accesso ai dati da parte di Paesi terzi, dovuto proprio all'esplosione dei servizi di *cloud computing* (i cui principali operatori sono, per l'appunto, domiciliati negli USA)[44].

L'aumentato carico di lavoro per l'ufficio dell'US Department of Justice (DOJ) ha comportato un repentino allungamento dei tempi necessari per completare i complessi adempimenti procedurali previsti dai vari trattati di mutua assistenza legale (MLAT), con il conseguente rischio di vanificare importanti indagini giudiziarie[45]: «The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world. While the MLAT process remains a critical evidence-gathering mechanism, the system has faced significant challenges keeping up with the increasing demands for electronic evidence in criminal investigations worldwide. Moreover, because many [Cloud Service Provider] move data among data storage centers in various countries, and

split up data into different pieces stored in different locations, it can be difficult both for governments and for the CSPs themselves to know where relevant data is located at any point in time for purposes of sending and fulfilling MLAT requests. The international community thus faces a critical question of how to provide governments efficient and effective access to evidence needed to protect public safety while preserving respect for sovereignty and privacy.»[46]

Due sono gli elementi essenziali del *Cloud Act*[47]. Il primo riguarda l'esplicito riconoscimento dell'applicabilità delle disposizioni dello SCA anche alle informazioni digitali conservate da fornitori di servizi *cloud* al di fuori del territorio USA. Ciò che conta è che il fornitore sia soggetto alla giurisdizione nazionale e abbia il possesso, la custodia o il controllo sui dati di cui si richiede la trasmissione: «A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.»

Per quanto, come si è accennato, tale previsione non abbia rappresentato di per sé una novità – in quanto il principio era già applicato da tempo dalla giurisprudenza prevalente, oltre che riconosciuto a livello internazionale dalla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[48] – la sua formalizzazione in un atto legislativo ha avuto se non altro il merito di aver reso esplicito l'atteggiamento del governo federale nei confronti degli operatori *cloud* domiciliati negli Stati Uniti, prevedendo al contempo alcune garanzie procedurali e sostanziali a tutela dei diritti dei cittadini e residenti USA, oltre che un meccanismo per contestare le richieste delle autorità federali (su cui subito *infra*).

Il secondo elemento è dato dalla previsione di un meccanismo basato su *executive agreement*, e dalla connessa definizione di *qualifying foreign government*. In particolare, il *Cloud Act* consente al governo USA di stipulare "accordi esecutivi" (*executive agreements*) bilaterali con Paesi terzi[49]. Questi accordi consentono ai Paesi firmatari di presentare, nell'ambito di indagini aventi ad oggetto *serious crimes*[50], richieste semplificate di accesso ai dati direttamente ai fornitori di servizi domiciliati negli Stati Uniti, secondo un meccanismo che andrebbe a completare, anziché a sostituire, le procedure attualmente previste dai trattati di assistenza giudiziaria esistenti.

Il *Cloud Act* introduce anche un meccanismo per consentire ai fornitori di servizi *cloud* di contestare (*quash*) le richieste delle autorità federali, qualora ricorrano due condizioni: il disvelamento delle informazioni può comportare per il fornitore il rischio concreto di violare un obbligo previsto dalla legislazione di un *qualifying foreign government*, e l'utilizzatore del servizio *cloud* non è un cittadino statunitense, né risiede negli Stati Uniti. Prima di accogliere la richiesta dell'operatore *cloud*, tuttavia, il giudice è chiamato a soppesare con attenzione tutti gli interessi in gioco nel caso specifico, alla luce di una serie di parametri indicati dallo stesso *Cloud Act* (la cosiddetta *comity analysis*)[51]. Nel prevedere una corsia preferenziale per i Paesi terzi che abbiano sottoscritto un *executive agreement* con gli Stati Uniti, il *Cloud Act* pone anche un importante limite a tutela dei cittadini e residenti USA. Per accedere ai dati di questi ultimi, infatti, il *Cloud Act* richiede il necessario ricorso ai tradizionali meccanismi previsti dagli accordi di mutua assistenza legale, ove esistenti.

Particolarmente interessante è la previsione del *Cloud Act* che esclude espressamente che gli *executive agreement* possano richiedere agli operatori *cloud* di decifrare i dati conservati sulla propria infrastruttura[52]. Questa previsione, che si pone in netta antitesi rispetto al timore del *going dark* che pure era alla base della stessa adozione del *Cloud Act*, è al tempo stesso un atto necessario per non danneggiare gli interessi economici degli operatori USA, e una vistosissima falla nell'intero meccanismo predisposto dal governo statunitense[53]. Non è un caso che, nelle pagine dedicate a illustrare l'impatto della nuova legislazione sulle loro politiche interne di protezione dei dati, i grandi operatori *cloud* d'oltreoceano – oltre a mettere ben in evidenza il loro costante impegno nell'opporsi alle richieste delle autorità ogni volta che ne ricorrano le condizioni – promuovano attivamente la cifratura quale strumento indispensabile per impedire l'accesso ai dati dei loro clienti da parte di "qualunque" soggetto terzo[54]. Del resto, la stessa elaborazione del modello di *Data Trust* illustrato nella prima parte di questo contributo è resa possibile, dal punto di vista tecnico, dall'applicazione generalizzata di algoritmi di cifratura sicuri.

Volendo tentare un primo bilancio degli effetti del *Cloud Act* sulla regolazione del fenomeno del *cloud computing*, gli aspetti negativi sembrano superiori ai benefici che il legislatore USA si proponeva di conseguire[55].

In primo luogo, nell'adottare un approccio unilaterale al fenomeno del *cloud computing* per garantire l'accesso alle informazioni da parte del governo USA, il *Cloud Act* ha finito per rafforzare le spinte ver-

so la localizzazione dei dati da parte di molti Stati, proprio quando uno dei fini perseguiti era dichiaratamente quello di evitare l'esacerbarsi dei conflitti legali, e della conseguente proliferazione di obblighi di localizzazione negli altri Paesi[56]. Anche gli operatori, dal canto loro, hanno in più occasioni mostrato di preferire un approccio "pragmatico" quando tratta di opporsi alle richieste delle pubbliche autorità nei Paesi nei quali offrono i loro servizi: in alcuni casi, hanno fatto leva sul principio di localizzazione per limitare l'accesso da parte delle autorità ai soli dati conservati sui *data center* del Paese richiedente. In altri casi, hanno mostrato di preferire il ricorso al criterio del controllo sui dati per opporsi a richieste provenienti da Paesi diversi dagli USA, nel quale erano domiciliati.

Inoltre, se è certamente vero che le procedure previste dagli accordi di mutua assistenza legale si sono dimostrate – proprio a causa della crescente diffusione di Internet, in generale, e dei servizi *cloud* in particolare – sempre più onerose in termini di tempo e risorse, è altrettanto vero che queste procedure erano state progettate segnatamente per offrire adeguate garanzie a tutela dei diritti e delle libertà fondamentali degli individui contro indebite intromissioni da parte dei pubblici poteri: «The rigorous procedures in the MLAT system are important safeguards for privacy and due process. When providing an alternative way, one would expect that the new regime would provide at least equivalent safeguards to those provided by the MLAT system. The CLOUD Act, however, removes some of the layers of protections provided by the MLAT system such as the rigorous reviews by [Department Of Justice], Attorney General, and courts without providing equivalent safeguards. Hence, bypassing the MLAT system could be faster for law enforcement, but it diminishes privacy standards. This is especially true for individuals in countries where there is no adequate privacy protection»[57].

In terzo luogo, nella sua pretesa di disciplinare con un unico tratto di penna un fenomeno così complesso e articolato, il *Cloud Act* omette completamente di regolare i rapporti tra i vari fornitori che compongono la "filiera" *cloud*. Come abbiamo evidenziato nella prima parte, una larghissima parte dei servizi *cloud* offerti sul mercato sono resi possibili dalla combinazione, verticale e orizzontale, di numerosi elementi infrastrutturali e applicativi messi a disposizione da una pluralità di operatori, ciascuno dei quali può avere un grado variabile di "possesso, custodia o controllo" sui dati[58]. In uno scenario di questo tipo, come scegliere il soggetto a cui inoltrare la richiesta di fornire i dati richiesti? Occorre privilegiare il livello infrastrutturale (dove i dati sono "fisicamente" conservati) o quello applicativo (tramite il quale sono generalmente acceduti)? Come vedremo nelle prossime pagine, il problema della definizione dei ruoli dei vari soggetti coinvolti nella fornitura di un servizio *cloud* all'utente finale non sono esclusive del *Cloud Act*, ma affliggono in maniera simile anche la normativa comunitaria.

8. L'accesso ai dati conservati sul *cloud*: la proposta di Regolamento *e-Evidence*

Nonostante tutti i suoi limiti, il *Cloud Act* ha contribuito a sollevare il velo su una questione di centrale importanza, ovvero il superamento del criterio dell'ubicazione fisica dei dati nel determinare la giurisdizione applicabile, in favore di un diverso principio, quello cioè del controllo sui dati. Al tempo stesso, ha mostrato tutti i limiti di un approccio unilaterale al fenomeno, che ha consentito agli operatori di sfruttare la babele di legislazioni nazionali (oltre che elementi di natura tecnica) per vanificare la pretesa di mantenere una qualche forma di controllo per finalità di interesse pubblico. Il problema rimane di estrema attualità anche nell'ambito dell'Unione europea, ed è alla base della recente proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[59].

Rispetto al *Cloud Act*, la proposta di regolamento mostra grande attenzione al problema delle garanzie, procedurali e sostanziali, a tutela dei diritti e delle libertà degli interessati, ma – allo stesso tempo e in modo analogo al *Cloud Act* – prende atto della portata dirompente dei modelli di distribuzione e gestione dei servizi e delle infrastrutture di *cloud computing* per dedurne l'inapplicabilità del criterio dell'ubicazione dei dati come base per affermare (o negare) la giurisdizione di uno Stato: «In molti casi i dati non sono più conservati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura *cloud* che consente in linea di massima l'accesso da qualsiasi luogo. I prestatori di servizi non hanno bisogno di essere stabiliti o avere server in ogni giurisdizione ma ricorrono piuttosto a un'amministrazione centralizzata e a sistemi decentrati per conservare i dati e fornire i servizi. In tal modo ottimizzano il bilanciamento del carico e riducono i tempi di risposta alle richieste di dati degli utenti. (...). Le imprese possono così fornire i contenuti dal server più vicino all'utente o in grado di inoltrare la comunicazione attraverso una rete meno congestionata»[60].

Per questo motivo, il Regolamento abbandona esplicitamente «il criterio di collegamento rappresentato dall'ubicazione dei dati, *poiché generalmente la conservazione dei dati non comporta alcun controllo da parte dello Stato nel cui territorio i dati sono conservati. Nella maggior parte dei casi il luogo di conservazione è determinato dal prestatore di servizi sulla base di considerazioni commerciali.*»[61].

Il Regolamento si applica ai servizi *cloud* e agli altri servizi di *hosting* che forniscono «una vasta gamma di risorse informatiche, quali reti, server o altre infrastrutture, mezzi di conservazione, app e servizi che permettono di conservare dati a diversi scopi»[62]. L'elemento decisivo per determinare se un servizio rientri o meno nell'ambito di applicazione del Regolamento è dato dalla conservazione dei dati, che deve rappresentare un momento essenziale del contratto di servizio: «I servizi per i quali la conservazione di dati *non è una componente propria* non sono contemplati dalla proposta. Sebbene la maggior parte dei servizi forniti dai prestatori comprenda qualche tipo di conservazione dei dati, specialmente quando sono forniti online a distanza, è possibile distinguere servizi per i quali la conservazione dei dati *non è una caratteristica principale bensì un elemento puramente accessorio*, quali servizi giuridici, architettonici, ingegneristici e contabili *forniti* online a distanza».

È facile immaginare come il criterio del carattere "non accessorio" della custodia dei dati sarà uno dei punti dolenti della normativa in sede di applicazione: oggigiorno, la conservazione dei dati per conto del titolare, anche nell'ambito dell'erogazione di servizi di natura professionale (si pensi ad esempio ai tantissimi servizi *cloud* utilizzati da aziende e privati per la contabilità, la gestione del personale, incluse le buste paga, la sicurezza sul lavoro, ecc.) rappresenta un elemento così comune dall'essere dato quasi per scontato. Al tempo stesso, si potrebbe anche obiettare che, nella fornitura di servizi IaaS e PaaS, la conservazione dei dati non rappresenta l'elemento principale, poiché lo scopo è quello di mettere a disposizione dell'utente una serie di risorse di natura logica, che questi è libero di utilizzare come meglio crede.

Ciò detto, la proposta di regolamento prevede due nuovi strumenti per la produzione e la conservazione dei dati che si rendono necessari nell'ambito di indagini o procedimenti penali: rispettivamente, gli ordini europei di produzione e gli ordini europei di conservazione. Entrambi gli ordini possono essere utilizzati per chiedere di produrre o conservare dati di cui il fornitore del servizio, situato in un'altra giurisdizione rispetto a quella dove gli ordini sono emessi, abbia la disponibilità. Tali ordini possono essere notificati direttamente al prestatore del servizio, e "sono eseguiti allo stesso modo degli ordini nazionali comparabili nella giurisdizione in cui il prestatore di servizi riceve l'ordine". Perché tali ordini siano validi, sono tuttavia necessarie alcune condizioni. In primo luogo, devono essere emessi o convalidati da un'autorità giudiziaria di uno Stato membro, previa valutazione della proporzionalità e necessità nel singolo caso, nell'ambito di un procedimento penale[63]. In secondo luogo, i dati di cui si richiede la conservazione o la produzione devono essere "necessari come prova in indagini o procedimenti penali". Devono cioè riferirsi a specifici autori, noti o sconosciuti, di un reato che è già stato commesso. In particolare, l'ordine europeo di conservazione consente di chiedere la conservazione solo di dati che sono già nella disponibilità del fornitore al momento della ricezione dell'ordine, e non di accedere a dati in una fase successiva alla ricezione dell'ordine stesso. In terzo luogo, gli ordini di produzione e conservazione possono essere emessi "solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione".

Il tema è, ancora una volta, troppo complesso e articolato per essere approfondito in questa sede nei suoi vari profili. Dalla particolare prospettiva di questo contributo, però, si deve segnalare come non sia sfuggita alla più attenta dottrina come, nella proposta di Regolamento, il tema della cifratura dei dati rappresenti (ancora una volta) il punto dolente in grado di vanificare l'intero edificio normativo messo in piedi dalla Commissione[64]. Nel Considerando n. 19 si legge infatti che i dati devono essere forniti dal prestatore di servizi "a prescindere dal fatto che siano criptati o meno". Mentre il *Cloud Act* esonera espressamente il fornitore del servizio dal comunicare alle autorità le chiavi di cifratura, nel caso del Regolamento la questione è assai più incerta, e dipende in ultima analisi da chi abbia il controllo sulle chiavi stesse. Se, come accade nella gran parte dei casi, le chiavi sono detenute dal fornitore del servizio, manca nel testo un'esplicita previsione che obblighi il rappresentante del *service provider* a produrre obbligatoriamente le chiavi di cifratura assieme ai dati cifrati, o quantomeno a produrre il testo decifrato mediante le chiavi in suo possesso. Si tratta di una lacuna tutt'altro che secondaria, anche considerato che molto spesso le chiavi sono detenute da soggetti stabiliti in Paesi terzi che, pur facendo capo al *service provider*, non coincidono con la società che rappresenta il *provider* nel territorio dell'Unione[65].

Nel caso in cui, invece, il fornitore utilizzi un sistema di cifratura c.d. *end-to-end*, la cifratura e la decifratura dei messaggi avviene interamente sui dispositivi degli utenti finali, con la conseguente im-

possibilità per i fornitori di accedere al contenuto dei messaggi perché, semplicemente, non dispongono delle relative chiavi. In questa ipotesi, l'acquisizione dei dati attraverso l'ordine europeo di produzione si rivelerebbe del tutto inutile. È stato quindi osservato che, qualora l'Unione europea «non trovi il modo di obbligare tutti i prestatori di servizi a consegnare i dati in chiaro per finalità di giustizia, indipendentemente dal sistema di criptazione utilizzato, i progressi investigativi nell'acquisizione transnazionale della prova elettronica non potranno che essere esigui e la sensazione potrebbe essere alla fine che la montagna avrà partorito un topolino»[66]. Tuttavia, se si considerano le caratteristiche "intrinseche" del *cloud computing* che abbiamo sin qui sommariamente evidenziato, è lecito dubitare che esista realmente una strada praticabile per raggiungere il risultato voluto. Del resto, il silenzio del Regolamento sul punto, che dedica alla cifratura solo uno scarso passaggio nel Considerando n. 19, dovrebbe essere emblematico proprio di tale difficoltà.

9. Riflessioni conclusive

Alla fine di questa lunga carrellata, peraltro non esaustiva, dei problemi che la regolazione del fenomeno *cloud* ha incontrato e incontra tutt'ora a livello nazionale e internazionale, si possono tentare alcune riflessioni.

Come abbiamo evidenziato più volte nel corso di questo contributo, molte delle difficoltà che si incontrano quando ci si appresta a regolare il fenomeno del *cloud computing* discendono dall'estrema eterogeneità dei servizi genericamente ricondotti sotto l'ombrello del *cloud*. Se è vero che questi servizi presentano alcuni tratti comuni (il carattere logico delle risorse utilizzate, la loro assegnazione in base alla domanda, la possibilità per l'utente di gestire tali risorse in autonomia tramite piattaforme eterogenee, ecc.), questi elementi non sempre offrono un "appiglio" sufficiente dal punto di vista della regolazione. Anche dal punto di vista dei modelli di servizio (IaaS, PaaS e SaaS, per limitarci alla classificazione tradizionale) e dei modelli di distribuzione (*cloud* pubblico, privato, comunitario e ibrido), le differenze sono tante e tali da rendere estremamente difficile ricostruire un quadro unitario. Se a tutto ciò si aggiungono anche le variazioni nei modelli di gestione dell'infrastruttura, e dei dati che su tali infrastrutture transitano o sono conservati (cha abbiamo riassunto, senza peraltro alcuna pretesa di completezza, nella tripartizione *Data Shard*, *Data Localization*, *Data Trust*), il quadro che ne emerge assomiglia più a un complicato mosaico, in cui soluzioni tecniche, organizzative e, non ultime, legali, si combinano in modi sempre diversi a seconda del contesto e delle esigenze.

Proprio perché il contesto è così complesso e – per certi versi – confuso, è necessario trovare alcuni punti fermi da cui partire per regolare un fenomeno che non può e non deve essere lasciato interamente alle scelte degli operatori *cloud*, poiché riguarda aspetti fondamentali della nascente "società dei dati".

Innanzitutto, occorre partire da un rilievo di natura concettuale. Secondo una concezione più tradizionale, i dati non sarebbero poi così diversi dagli altri beni intangibili, come il denaro, e che il *cloud* in fondo sia poco più del metallo e dei bulloni che ne compongono l'hardware: «Despite the technological wizardry of modern life, the 'cloud' is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries.»[67]

Ovviamente, non c'è alcuna *wizardry* nelle modalità di funzionamento del *cloud* e, più in generale, di Internet. Tuttavia, se è vero che alla fine qualunque tecnologia può essere ridotta a una massa di server, dischi, cavi e altri apparecchi fisici, è anche vero che le "pratiche" che tali oggetti abilitano (si pensi, oggi, alle possibilità offerte dalle *blockchain*, dall'*Internet of Things* e agli sviluppi dell'intelligenza artificiale, solo per fare degli esempi) impongono di adottare un atteggiamento non riduzionista, e non unilaterale, in grado di guardare ai fenomeni nella loro complessità. Lo stesso vale, a maggior ragione, per i dati che su queste infrastrutture transitano. Discutere se, dal punto di vista dell'applicazione di istituti e norme giuridiche, questi presentino analogie con il denaro o con altri beni intangibili rischia di tradursi, almeno ad avviso di chi scrive, in un mero esercizio di stile. Se non altro, perché sono proprio i beni intangibili come la moneta o il debito ad andare incontro a vere e proprie "mutazioni genetiche" a seguito dell'erompere di nuove tecnologie "abilitanti" (si pensi al crescente peso acquisito dalle criptovalute come Bitcoin), e non viceversa.

Ciò è particolarmente vero quando si discute degli obblighi di localizzazione dei dati all'interno dei confini nazionali. Che la loro previsione possa essere sufficiente, "di per sé", a soddisfare le spesso contrastanti esigenze pubbliche legate alla disponibilità dei dati (inclusa la possibilità di sottoporre a sequestro i server su cui i dati sono conservati) non tiene in debito conto né la natura composita e al tempo stes-

so fluida di Internet, né delle possibilità tecnologiche che possono rendere vana qualsiasi pretesa di accesso ai dati per l'esercizio di pubblici poteri, né – e questo è forse la lezione più importante impartita dal *Cloud Act* – delle possibili "reazioni" a catena che tali previsioni possono innescare da parte dei vari soggetti coinvolti, sia pubblici che privati (lo dimostra in modo esemplare il modello di *Data Trust* elaborato da Microsoft come risposta al *Cloud Act*).

Entrambi gli obiettivi perseguiti dal *Cloud Act*, ovvero ridurre il proliferare di obblighi di localizzazione a livello internazionale mediante la conclusione di accordi bilaterali, e assicurare alle autorità federali la possibilità di poter continuare ad accedere ai dati necessari all'esercizio delle funzioni pubbliche, possono dirsi falliti. Al tempo stesso, però, proprio il *Cloud Act* ha mostrato i limiti del criterio basato sul possesso, custodia o controllo dei dati, mediante il quale si cerca di agire sui fornitori di servizi *cloud* affinché siano questi ad attivarsi per rendere disponibili i dati dei propri utenti conservati – o, il più delle volte, sparsi – sulla loro infrastruttura globale, a prescindere dalla loro ubicazione geografica. A non funzionare, in questo caso, è stato soprattutto l'approccio unilaterale al fenomeno (oltre che una generale sottovalutazione della complessità della filiera *cloud*), che ha consentito ai grandi operatori di fare quello che di solito tendono a fare in casi simili: sfruttare la frammentazione delle legislazioni nazionali a loro vantaggio, in questo caso specifico per "spogliarsi", nella forma e nella sostanza, di qualunque controllo sui dati.

Molto meglio allora partire dalla particolare combinazione di elementi giuridici, organizzativi e tecnici alla base del modello di "Data Trust" per affrontare seriamente il problema della "sovranità dei dati". Indipendentemente dalle questioni circa la riproducibilità e la scalabilità dell'esperimento tedesco, l'introduzione del principio di separazione della "gestione dell'infrastruttura" rispetto alle questioni legate all'accesso ai dati potrebbe rivelarsi, con gli opportuni adattamenti, una delle chiavi di lettura di un futuro assetto europeo della regolamentazione sul *cloud*. Questa distinzione, del resto, la si ritrova anche all'interno del progetto di *cloud* franco-tedesco, oggetto di analisi all'interno di questo stesso volume. Come è stato osservato, infatti, nella documentazione di GAIA-X "vengono utilizzati sia il termine *data sovereignty* che *digital sovereignty*. Mentre la sovranità digitale viene definita come il potere di decidere «about how digital processes, infrastructures and the movement of data are structured, built and managed», la *data sovereignty* viene presentata come un particolare aspetto della sovranità digitale, consistente nel pieno controllo del *data owner* rispetto alla collocazione e all'uso dei dati. La sovranità sui dati sarebbe dunque il primo passo per assicurare una sovranità digitale piena"[68].

Note

[1]Nel 2020 il mercato mondiale dei servizi *cloud* ha raggiunto i 371.4 miliardi di dollari. Anche per effetto della recente pandemia di COVID-19, si stima che nel 2025 il mercato ammonterà a 832 miliardi di dollari, con un tasso di crescita annuo del 17.5% (fonte: *Research and Markets*).

[2]Per una sistematica revisione delle misure di localizzazione adottate a livello mondiale si vedano A. Chander, U.P. Le, *Data Nationalism*, in "Emory Law Journal", 2015, n. 3, p. 677-739; Organisation for Economic Co-operation and Development, *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL.

[3]Sulle vicende legate alla piattaforma "Immuni" si veda V. Pagnanelli, *Immuni: spunti per una riflessione privacy-oriented*, in "Questione Giustizia", maggio 2020.

[4]A. Chander, U.P. Le, *op. cit.*, p. 679.

[5]Per una disamina degli effetti negativi delle misure di localizzazione sulla sicurezza e la concorrenza si vedano, fra i tanti, J. Selby, *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?*, in "International Journal of Law and Information Technology", 2017, n. 3, p. 213-232; H. Brehmer, *Data Localization: the unintended consequences of privacy litigation*, in "American University Law Review", 2018, n. 3, p. 927-969; R. Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and other Online Activities*, National Telecommunications and Information Administration, 2016; J. Lenhart, *Security for the 21st Century Economy: Borders Hold Less Meaning – and That's a Good Thing*, Information Technology Industry Council, 2017.

[6]Fonte: *Statista*. Dati riferiti ad aprile 2020.

[7]Sulla storia e l'evoluzione del *cloud computing* si vedano, tra i tanti, M.S. Gendron, *Business Intelligence and the Cloud*, John Wiley & Sons, 2014; V.V. Arutyunov, *Cloud Computing: Its History of Development, Modern State, and Future Considerations*, in "Scientific and Technical Information Processing", 2012, n. 3, p. 173-178.

[8]A. Regalado, *Who coined "Cloud computing"?*, in "MIT Technology Review", 31 ottobre 2011.

[9]NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, 9 December 2011, Special publication n. 800-144, p. IV. Definire il fenomeno in modo univoco è difficile per almeno due ragioni: «First, as there is no clear difference between the cloud and the Internet itself, any attempt to create a legal distinction among various online services will invariably lead to legal "overreach" with unintended consequences. Second, forcing such a distinction is likely to mislead the very consumers that the legislation is intended to protect because they might wrongly think that a particular rule, regulation, or practice will protect them so long as the services they are using are labeled as cloud services» (Cfr. P.S. Ryan, S. Falvey, R. Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, in "Computer", 2013, n. 12, p. 55.

[10]I limiti propri di qualunque definizione sono del resto stati messi in evidenza dallo stesso NIST: «Much of what has been written about cloud computing is definitional, aimed at identifying important paradigms of deployment and use, and providing a general taxonomy for conceptualizing important

facets of service». Cfr. NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, cit., p. 3).

[11] «Cloud computing can be considered a new computing paradigm insofar as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. Because of the implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention», *ibidem*.

[12] NIST, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, September 2011, Special publication n. 800-145.

[13] Per "scalabilità" si intende la capacità di un sistema di aumentare o diminuire le proprie prestazioni (e dunque il carico di lavoro che è in grado di svolgere nella stessa unità di tempo) in funzione della necessità e della disponibilità. La scalabilità si distingue in "orizzontale" e "verticale". La prima è la capacità di aumentare la capacità di lavoro sfruttando più componenti hardware o software in modo che funzionino come una singola unità logica (in pratica, il lavoro viene suddiviso tra più sistemi, ciascuno dei quali in grado di operare autonomamente). La scalabilità verticale, invece, aumenta la capacità aggiungendo più risorse a una stessa unità (ad esempio, aggiungendo nuova memoria o dischi più capienti, aumentando il numero di processori, ecc.). Mentre prima della diffusione del *cloud* la scalabilità poteva essere ottenuta solo comprando o noleggiando ulteriori componenti hardware e software, e dunque solo a seguito di un'attenta pianificazione e a fronte di notevoli investimenti, i servizi *cloud* possono essere scalati "elasticamente", ossia in base all'andamento (in tempo reale) del carico di lavoro. Il che significa anche che, una volta che il carico diminuisce, è possibile ridurre l'erogazione delle risorse in eccesso e, cosa assai rilevante, smettere di pagare per ciò che non si usa.

[14] Per chiarire meglio l'impatto dei modelli di *cloud computing*, si può immaginare il caso di un'azienda che decida di vendere i propri prodotti sul web. Prima dell'avvento dei servizi *cloud*, per realizzare e ospitare sulla propria infrastruttura un sito di *e-commerce* avrebbe dovuto preoccuparsi di tutta la "filiera" tecnologica: l'acquisto, l'installazione e la configurazione di server, *firewall*, *load balancer* e apparati di rete, nonché della predisposizione di adeguate misure di sicurezza fisica (sale adeguate, impianti di condizionamento, sistemi antincendio, ecc.) e logica (DMZ, sistemi di autenticazione, monitoraggio del traffico di rete, ecc.), la configurazione degli ambienti di produzione e di test, l'acquisto delle licenze software necessarie, e tantissimi altri aspetti. Nel decidere il tipo di hardware da acquistare (numero di processori, memoria, spazio disco, ecc.), l'azienda avrebbe dovuto stimare accuratamente non il carico di lavoro "medio", ma quello massimo ipotizzabile. Il carico di lavoro di un servizio web, infatti, non è mai costante: periodi di bassa e moderata attività (ad esempio durante le ore notturne) si alternano a picchi di lavoro più o meno intensi che possono mettere a dura prova le risorse disponibili (si pensi, per esempio, al periodo natalizio o ai sempre più frequenti saldi promossi online). Se queste risorse non sono sufficienti per far fronte alle richieste in un certo momento, una parte di queste richieste non potrà essere servita, causando disservizi e malumori agli utenti, o addirittura malfunzionamenti del sistema. Al tempo stesso, durante i periodi di inattività o di "scarico", tutte le risorse in eccesso, acquistate solo per poter far fronte ai momenti di picco, sono destinate a rimanere inutilizzate, nonostante siano state investite somme ingenti per acquistarle. È vero che un'azienda avrebbe potuto noleggiare tutto il necessario, anziché acquistarlo in proprio, ma anche in questo caso la "rigidità" del sistema rimarrebbe sostanzialmente inalterata e i costi largamente fissi. Grazie al *cloud*, invece, l'azienda può concentrarsi su ciò che le interessa davvero, ossia vendere i propri prodotti sul web, senza doversi preoccupare di acquistare (o noleggiare) e configurare le risorse necessarie. Queste possono essere create, aggiunte o ridimensionate in tempo reale, per seguire l'andamento del carico di lavoro e, una volta che non sono più necessarie, possono essere dismesse in tutta facilità, smettendo così di pagare per ciò che non viene utilizzato.

[15] Il confine tra IaaS e PaaS, relativamente netto in teoria, nella pratica è andato sempre più sfumando, sia perché i primi offrono oggi funzionalità di alto livello, come ad esempio macchine virtuali già preconfigurate per poter svolgere un numero sempre crescente di compiti; sia perché i servizi PaaS tendono a permettere all'utente che lo desideri un controllo più granulare sulle caratteristiche della sottostante infrastruttura virtuale.

[16] Per una "carrellata" sui diversi modelli di servizio si rinvia a A. Biasiotti, *Il nuovo regolamento europeo sulla protezione dei dati*, EPC Editore, 2018, p. 723 ss.

[17] Questa affermazione deve essere presa con le dovute cautele, poiché sempre più spesso anche i servizi infrastrutturali e/o di piattaforma prevedono (si potrebbe dire "per impostazione predefinita") forme di cifratura dei dati, in transito o "a riposo", che permettono di assicurare già in partenza un livello di sicurezza piuttosto elevato, salva la possibilità per l'utente di applicare misure ulteriori per soddisfare requisiti di sicurezza più stringenti.

[18] In informatica, l'aggettivo "trasparente" ha un significato diverso dal linguaggio comune, indicando un processo che si svolge senza che l'utente ne sia consapevole e senza che a quest'ultimo sia richiesto alcun tipo di intervento. Ad esempio, una modifica che attiene al modo con cui un software salva e organizza i dati è "trasparente" rispetto all'utente finale se, dal punto di vista di quest'ultimo, il software continua a operare come prima, senza che vi siano cambiamenti nell'interfaccia utente o nei flussi di lavoro, che rimangono quelli soliti ai quali l'utente è abituato.

[19] Nel 2017 Dropbox ha avviato la migrazione di gran parte dei suoi sistemi dall'infrastruttura di AWS sui propri *data center*.

[20] Fonte: *Mordor Intelligence*.

[21] V.V. Arutyunov, *op. cit.*

[22] In merito alla strategia italiana per l'adozione dei servizi *cloud* nell'ambito delle Pubbliche Amministrazioni si veda V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in questo fascicolo.

[23] P.M. Schwartz, *Legal Access to the Global Cloud*, in "Columbia Law Review", 2018, n. 6, p. 1681-1762.

[24] Esistono almeno tre diverse strategie di partizionamento dei dati. Nel partizionamento "orizzontale" (quello chiamato propriamente *sharding*), ogni partizione ha lo stesso schema di tutte le altre, ossia contiene le stesse tipologie di dati (ad esempio, gli ordini dei clienti). Nel partizionamento "verticale", invece, ogni partizione contiene un particolare sottoinsieme dei dati archiviati, suddivisi in base al loro modello di utilizzo. In questo modo, i dati utilizzati più spesso possono essere collocati in una partizione verticale, mentre quelli usati raramente possono essere collocati in un'altra partizione. Infine, nel partizionamento "funzionale", dati sono aggregati in base alla loro modalità di utilizzo: in un sistema di *e-commerce*, ad esempio, i dati delle fatture potrebbero essere archiviati in una partizione dedicata all'area amministrativa, e quelli relativi all'inventario dei prodotti in magazzino in un'altra partizione, pronti per essere utilizzati dalla logistica e dalle vendite.

[25] In un server, la quantità di spazio di archiviazione su disco è in genere limitata, ma è possibile sostituire i dischi esistenti con versioni più capienti o aggiungere altri dischi man mano

che i volumi di dati aumentano. Tuttavia, il sistema finirà prima o poi per raggiungere un limite oltre al quale non è più possibile aumentare la capacità di archiviazione, se non a costi proibitivi. Allo stesso modo, un singolo server che ospita tutti i dati potrebbe non essere in grado di fornire la potenza di calcolo necessaria per servire le interrogazioni (*query*) degli utenti, con conseguente aumento dei tempi di risposta e frequenti errori dovuti all'indisponibilità delle risorse. Anche in questo caso potrebbe essere possibile aggiungere ulteriore capacità computazionale e/o memoria, ma il sistema raggiungerà comunque un limite quando non sarà possibile aumentare ulteriormente le risorse di calcolo. Infine, c'è da considerare la larghezza di banda della rete. Anche in questo caso, infatti, un elevato numero di richieste aventi ad oggetto grandi quantità di dati possono generare un traffico di rete superiore alla capacità della rete usata per la connessione al server, con conseguente aumento dei tempi di risposta ed errori.

[26] P.M. Schwartz, *op. cit.*, p. 1965.

[27] Per maggiori informazioni sulla complessiva infrastruttura di Amazon Web Services, si veda "Regioni e zone di disponibilità". Anche l'infrastruttura *cloud* di Microsoft Azure prevede un'articolazione simile; per maggiori informazioni si veda "Azure geographies".

[28] Timori peraltro non infondati, se solo si pensa al caso "Snowden" e all'acuirsi delle tensioni tra l'Unione europea e gli Stati Uniti. Per un approfondimento delle vicende si rinvia a E.J. Snowden, *Errore di sistema*, Longanesi, 2019.

[29] Riconosciuto nel nostro ordinamento grazie alla l. 16 ottobre 1989, n. 364, con cui è stata ratificata la Convenzione dell'Aja sulla legge applicabile ai *trusts* e sul loro riconoscimento, adottata da L'Aja il 1° luglio 1985.

[30] *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. 2016), 14 July 2016.

[31] Oltre al contenuto delle e-mail riconducibili a un determinato *account* di posta elettronica, l'ordine includeva anche la produzione di ulteriori informazioni collegate a detto *account*, conservate sui server della sede americana. Queste informazioni sono sostanzialmente di tre tipi: «First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database». *Ivi*, p. 9.

[32] Tale scelta dipendeva peraltro da esigenze di natura tecnica (*in primis* diminuire il tempo di latenza portando i dati più vicino al luogo di accesso), non quello di soddisfare particolari esigenze di localizzazione.

[33] *Microsoft Corp. v. United States*, cit., p. 20.

[34] *Ivi*, p. 7.

[35] D. Callaway, L. Determan, *The New US Cloud Act. History, Rules, and Effects*, in "The Computer & Internet Lawyer", 2018, n. 8.

[36] A riprova del carattere "eccezionale" del caso *Microsoft Ireland* si vedano anche i casi *Yahoo Winsconsin*, *Yahoo Florida* e *Google California*, tutti successivi al primo, nei quali viene riaffermato il principio per cui le disposizioni dello SCA trovano applicazione a prescindere dal luogo in cui sono ubicati i dati.

[37] P.M. Schwartz, *op. cit.*, p. 1685 ss.

[38] *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (2017).

[39] *Ivi*, p. 25-26.

[40] *Ibidem*.

[41] In argomento si vedano le considerazioni di D. Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE, May 22, 2017.

[42] *Ibidem*.

[43] P.M. Schwartz, *op. cit.*, p. 1681-1762.

[44] Oggi circa l'85% delle indagini di polizia si basa su elementi di prova digitali, e in due terzi di questi casi vi è la necessità di richiedere tali elementi a fornitori di servizi *cloud* localizzati in altre giurisdizioni. Il numero di richieste verso i principali operatori è cresciuto dell'84% in soli cinque anni (2013-2018). Dati della Commissione europea.

[45] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, April 2019.

[46] *Ibidem*.

[47] Per approfondimenti sul *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* si vedano, tra i tanti, J. Galbraith, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, in "American Journal of International Law", 2018, n. 3, p. 487-493; D. Callaway, L. Determan, *op. cit.*

[48] Si veda in particolare l'art. 18 della Convenzione, in base al quale «Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control (...)».

[49] Perché possa essere concluso un *executive agreement* con un Paese terzo, il *Cloud Act* prevede che l'*Attorney General*, assieme al Segretario di Stato, verifichino e certifichino in forma scritta al Congresso USA che la legislazione del Paese terzo offra «robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement».

[50] Sino ad oggi, l'unico accordo sottoscritto dal governo USA è quello con la Gran Bretagna. Nel testo viene chiarito che, per *serious crime* si intende, ai sensi dell'art. 1, n. 14, dell'accordo, qualunque reato che preveda come massimo edittale almeno tre anni di reclusione («Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years»). Cfr. l'*executive agreement*.

[51] Ai sensi dell'articolo 2713 dello SCA (come emendato dal *Cloud Act*) gli elementi che devono essere tenuti in considerazione dalla corte nel decidere sulla richiesta di *quash* sono i seguenti: «a) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure; b) the interests of the qualifying foreign government in preventing any prohibited disclosure; c) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; d) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; e) the nature and extent of the provider's ties to and presence in the United States; f) the importance to the investigation of the information required to be disclosed; g) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and h) if the legal process has been sought on behalf of a foreign authority pursuant to sec-

tion 3512, the investigative interests of the foreign authority making the request for assistance».

[52]18 U.S. Code § 2523 (b) (3): «the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data».

[53]Falla da cui, come si vedrà più avanti, non è esente neppure la proposta di Regolamento europeo relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*). Il tema della crittografia, in particolare quella c.d. *end-to-end* (nel quale solo gli utenti che stanno comunicando sono in grado di leggere i messaggi, ad esclusione di qualsiasi altro soggetto, incluso il fornitore del servizio) è tornata di recente sotto i riflettori a seguito della presentazione di due proposte di legge, al momento entrambe all'esame del Senato USA. La prima proposta, denominata *Lawful Access to Encrypted Data Act* (o *LEAD Act*), mira a obbligare i fornitori di dispositivi e di servizi internet a decifrare i dati e a metterli a disposizione delle autorità in forma intellegibile. In questo senso, la proposta «is an actual, overt, make-no-mistake, crystal-clear ban on providers from offering end-to-end encryption in online services, from offering encrypted devices that cannot be unlocked for law enforcement, and indeed from offering any encryption that does not build in a means of decrypting data for law enforcement» (R. Pfefferkorn, *There is now an even worse anti-encryption bill than EARN IT. That doesn't make the EARN IT bill ok*, in The Center for Internet and Society, Stanford Law School, 24 giugno 2020). La seconda proposta di legge, l'*Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (il c.d. *EARN IT Act*) pone una serie di ostacoli, per lo più indiretti, al ricorso alle tecniche di crittografia per proteggere i contenuti.

[54]Si consideri, a titolo di esempio, quanto riportato nella documentazione ufficiale di Amazon Web Services: «In the event we cannot resolve a dispute, we do not hesitate to go to court. Amazon has a history of formally challenging government requests for customer information that we believe are overbroad or otherwise inappropriate. We will continue to resist requests, including those that conflict with local law such as GDPR in the European Union, to do everything we can to protect customer data. We will also continue to notify customers before disclosing content, and we provide advanced encryption and key management services that customers can use to protect their content further. We have industry leading encryption services that give our customers a range of options to encrypt data in-transit and at rest, and to manage encryption/decryption keys – because encrypted content is rendered useless without the applicable decryption keys».

[55] Per una disamina approfondita del Cloud Act si vedano, tra i tanti, P.M. Schwartz, *op. cit.*, p. 1748 ss.; D. Callaway, L. Determan, *op. cit.*

[56]Si veda la lettera inviata da Peter J. Kadzik, *Assistant Attorney General* presso il Dipartimento di Giustizia USA, al presidente del Senato Joseph R. Biden (luglio 2016): «The current situation is unsustainable. Some countries have begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees. If foreign governments cannot access data, they need for legitimate law enforcement, including terrorism investigations, they may also enact laws requiring companies to store data in their territory. Such data localization requirements would only exacerbate conflicts of law, make Internet enabled communications services less efficient, threaten important commercial interests, undermine privacy protections by requiring data storage in jurisdictions with laws less protective than ours, and ultimately impede U.S.-government access to data for its investigations. And as the global market for Internet related services expands, the U.S. government will increasingly need effective and efficient access to electronic information stored or uniquely accessible abroad. Conflicts of law may increasingly pose an obstacle to such access».

[57]H.H. Abraha, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, in "International Data Privacy Law", 2019, n. 3, p. 213. Proprio per ovviare alle evidenti inefficienze dell'attuale sistema basato sull'accordo di mutua assistenza legale del 2001 tra Stati Uniti e Unione europea, rafforzando al contempo gli standard di protezione dei diritti degli interessati, il Comitato europeo per la protezione dei dati personali ha sottolineato l'urgenza di ridisegnare l'intero processo per dar vita a una "nuova generazione" di accordi: «The Mutual Legal Assistance Treaty already in force between the EU and the US, as a legal instrument mainly aimed at facilitating judicial cooperation, contains only very limited provisions relevant from a data protection point of view. The EDPB and EDPS therefore wish to emphasize the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation. In addition, the "dual criminality principle" providing safeguard against discrepancy between how a crime is defined under the foreign law and how the same crime is legally defined under EU law should be preserved» (EDPB, *LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, 10 luglio 2019).

[58]H.H. Abraha, *op. cit.*, p. 208: «In the cloud computing environment, 'the delivery of cloud services often depends on complex, multi-layered arrangements between various providers.' This means that different providers can be involved in a particular cloud service offering with different degrees of control over the underlying technologies and stored data. This complicates the task of law enforcement agencies in identifying who is in 'possession, custody, or control' of personal data in view of serving a subsequent order. The consequence is that the CLOUD Act may target service providers (such as Infrastructure Service providers) who do not have effective 'possession, custody, or control' over the sought-after data. In this regard, one would argue that the CLOUD Act is not compatible with some business and technological realities of cloud computing».

[59]Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, 2018/0108.

[60]*Ibidem*. Si osserva inoltre che «Dato che internet non conosce frontiere, tali servizi possono essere prestati da qualsiasi luogo del mondo e non richiedono necessariamente un'infrastruttura fisica né la presenza di un'azienda o di personale negli Stati membri in cui sono offerti o nel mercato interno nel suo insieme. Non richiedono nemmeno un luogo specifico in cui conservare i dati: spesso il prestatore di servizi sceglie tale luogo in base a considerazioni legittime quali la sicurezza dei dati, le economie di scala e la rapidità di accesso. Di conseguenza, in un numero crescente di procedimenti penali riguardanti qualsiasi tipo di reato, le autorità degli Stati membri richiedono l'accesso ai dati che potrebbero servire da prove e che sono conservati al di fuori del loro paese e/o da prestatori di servizi situati in altri Stati membri o in paesi terzi».

[61]*Ibidem*, nostro il corsivo.

[62]Il Regolamento si applica anche «ai mercati digitali che consentono ai consumatori e/o alle imprese di concludere operazioni tramite contratti di vendita o di servizi online. Tali operazioni sono effettuate o sul sito web del mercato online o sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online. È pertanto questo mercato che generalmente detiene prove elettroniche che possono essere necessarie nel corso di procedimenti penali».

[63]Si intende dalla fase preprocessuale delle indagini preliminari fino alla chiusura del procedimento con sentenza o altra decisione. Il regolamento opera anche una distinzione tra (meta) dati relativi agli accessi e quelli relativi al contenuto dei dati stessi: «gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi per qualsiasi reato, mentre quelli per la produzione di dati relativi alle operazioni o al contenuto possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati precisati nella proposta e se vi è un collegamento specifico con gli strumenti elettronici e i reati rientranti nel campo di applicazione della direttiva (UE) 2017/541 sulla lotta contro il terrorismo».

[64]Sul punto si rinvia all'approfondita analisi e alle acute osservazioni di R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa della Commissione europea al vaglio del Consiglio dell'Unione*, in "Diritto Penale Contemporaneo", 2019, n. 1, p. 71 ss., da cui sono tratte le considerazioni che seguono.

[65]Sul punto cfr. R. Pezzuto, *op. cit.*, in part. pp. 73-74.

[66]*Ibidem*, p. 74.

[67]A.K. Woods, *Against Data Exceptionalism*, in "Stanford Law Review", 2016, n. 4, p. 729.

[68]V. Pagnanelli, *op. cit.*

* * *

Cloud computing: technical models and legal frameworks

Abstract: The cloud computing market has experienced an exponential growth rate in recent years, which the recent global pandemic emergency will eventually strengthen further. The success of this complex and varied "ecosystem" of technologies and services lies in a synergistic combination of factors, as well as the increasingly widespread diffusion of smartphones and tablets, which has led to new ways of using IT services. Cloud platforms today perform an enabling function with respect to a practically infinite variety of services, which could not exist without the resources made available by cloud computing providers. From a legal point of view, however, cloud computing leaves enormous questions still largely unresolved. How to protect the rights of data subjects when their data can be moved, unpacked, recomposed and replicated in any node of the global network with a simple click? How to regulate such kaleidoscope of different services and how to share obligations and responsibilities among the various subjects that make up the cloud supply chain? In many respects, the approach followed by the United States and the European Union could not be more different, but both pretend to unilaterally regulate a phenomenon - cloud computing and, more generally speaking, the Internet - in which "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Keywords: Cloud computing – Cloud Act – e-Evidence Regulation

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0021

La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa

Stefano Torregiani*

L'incremento esponenziale della circolazione dei dati dovuto all'avvento della digitalizzazione è stato accompagnato da un altrettanto rilevante aumento degli obblighi di localizzazione delle informazioni imposti dagli Stati membri dell'Unione europea. Il legislatore continentale, conscio dell'importanza che il libero flusso delle informazioni ricopre per la realizzazione del mercato unico digitale, ha reagito all'espansione dalla *data localization* attraverso una serie di interventi particolari e distinti, prevalentemente fondati sulla distinzione, non ancora del tutto pacifica, tra dati personali e dati non personali. Attraverso l'analisi delle similitudini e delle differenze che caratterizzano le principali fonti dell'ordinamento europeo in materia di dati, lo scopo del presente lavoro sarà quello di valutare se questo mosaico regolamentare, preferito ad un approccio onnicomprensivo, sia idoneo a disciplinare efficacemente lo spazio comune europeo dei dati.

Circolazione dei dati – Obblighi di localizzazione – Dato personale – Dato non personale

Sommario: *1. Introduzione – 2. La reazione europea alla* data localization *– 3. La circolazione dei dati personali – 3.1. All'interno dell'Unione europea – 3.2. Al di fuori dell'Unione europea – 4. La circolazione dei dati non personali – 4.1. Il divieto degli obblighi di localizzazione – 4.2. Una nuova portabilità autoregolamentata – 5. I punti deboli dell'impianto regolamentare europeo – 6. La necessità di una visione onnicomprensiva per la realtà digitale moderna*

1. Introduzione

Il fenomeno della data driven innovation è diventato l'indiscusso protagonista dell'attuale realtà economica e sociale nel giro di pochissimi anni, trasformandosi nel punto di riferimento per qualsiasi modello di sviluppo economico e tecnologico. Attualmente, il vero potere si trova nelle mani di chi, tramite la gestione di una vastissima mole di dati, riesce ad estrarre valore e, conseguentemente, prendere decisioni economicamente molto vantaggiose, a fronte di costi assai ridotti[1].

Questo è il principale motivo alla base della repentina acquisizione di rilevanza da parte del bene "dato", il quale oggi si presenta come una risorsa economico-finanziaria di cui nessuna attività, né pubblica, né privata, può più fare a meno[2].

Uno degli aspetti più importanti concernenti l'innovazione digitale è quello relativo alla circolazione di queste informazioni: l'addestramento degli algoritmi, le analisi di mercato, l'elaborazione di strategie pubbliche, l'adozione di piani aziendali sono tutte attività che hanno come denominatore comune la stretta correlazione con il trattamento di una serie di dati che provengono da fonti diverse e, nella maggior parte dei casi, da Paesi diversi. In tal senso, dunque, la tematica del flusso di dati gioca un ruolo chiave in una realtà economico-giuridica che si contraddistingue per la sua globalità e per la rilevante presenza di catene di valore transfrontaliere[3].

Tuttavia, parallelamente alla diffusione dei dati ed alla loro circolazione, l'ultima decade ha registrato la proliferazione del suo antagonista, gli obblighi di localizzazione (fenomeno internazionalmente co-

*S. Torregiani è dottorando di ricerca in Scienze giuridiche presso l'Università degli Studi di Macerata nel curriculum Istituzioni e territorio nella dimensione nazionale, europea e internazionale. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

nosciuto con il nome di *data localization*)[4]. Il loro numero è cresciuto di pari passo all'aumento dell'importanza dei dati per la società, giacché anche il dato risponde all'antica logica secondo cui più un bene ha valore, più è incline al rischio di offesa e, di conseguenza, richiede una maggiore tutela. Difatti, le principali ragioni che sono alla base dell'introduzione di misure legislative o amministrative da parte degli Stati a difesa del proprio patrimonio informativo riguardano la sicurezza interna, la facilità di accesso delle autorità nazionali alle informazioni necessarie alla vigilanza e lo sviluppo industriale domestico[5].

L'obiettivo del presente contributo è quello di valutare come le due tematiche interconnesse, ma contrapposte, della libera circolazione e della *data localization* siano state affrontate dal legislatore europeo tramite gli ultimi interventi in materia di *data law*. Come si avrà modo di vedere nel prosieguo, anziché affrontare il problema proponendo una soluzione unica ed onnicomprensiva, l'Unione europea ha preferito prima effettuare una distinzione di fondo tra dato personale e dato non personale per poi procedere all'adozione di due normative distinte che, malgrado comunicanti, rischiano di scostarsi troppo da una realtà digitale in cui tale distinzione è molto meno chiara di quanto la normativa lasci presupporre[6].

2. La reazione europea alla *data localization*

Di regola, con il termine *data localization* non ci si riferisce solo ed esclusivamente a quelle misure che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento, poiché vengono ricomprese anche quelle disposizioni che fissano vincoli più o meno stringenti al trasferimento dei dati al di là dei confini nazionali[7]. Questa circostanza allarga enormemente il novero delle misure che possono rientrare nella definizione, coprendo sostanzialmente tutti gli ordinamenti che hanno una disciplina in materia di circolazione dei dati, in quanto, quando non impongono un divieto generale oppure permettono il trasferimento solo dopo un primo trattamento a livello locale[8], si premurano comunque di prescrivere una serie di condizioni affinché i dati possano abbandonare il territorio di provenienza.

Alla luce di queste considerazioni, le restrizioni alla libera circolazione possono distinguersi in "rigide" o "condizionali"[9]. Le prime, le quali obbligano il titolare ad eseguire una determinata fase del trattamento localmente, si suddividono a loro volta in sottocategorie, a seconda della rigidità della misura: partendo da una disposizione che richiede il solo storage a livello locale – ossia mantenere una copia interna – e passando per quelle che, oltre all'archiviazione, impongono il processing domestico, si arriva fino al divieto generale di trasferimento, con la conseguenza che, al di fuori dei propri confini, è vietato persino il semplice accesso alle informazioni[10]. Le restrizioni condizionali, invece, lasciano sempre uno spazio, più o meno angusto, al trasferimento, ma lo rendono più gravoso giacché alcuni requisiti devono essere soddisfatti dal soggetto trasferente o dal ricevente, oppure da entrambi[11]. Tale distinzione si riflette anche sul bersaglio delle restrizioni: mentre quelle condizionali sono concepite al fine di limitare i trasferimenti di un determinato tipo di dato – generalmente personale –, quelle rigide hanno una dimensione prettamente settoriale, con la conseguenza che la distinzione tra dato personale e non personale non acquisisce alcuna rilevanza[12].

A dispetto dell'incremento massivo, la dottrina è sostanzialmente concorde nel valutare come negativi gli effetti prodotti dalla *data localization* nei confronti delle economie statali, giacché gli obiettivi di sicurezza, controllo e privacy che sono alla base dell'introduzione di simili misure restrittive potrebbero essere raggiunti tramite strade alternative capaci di apportare incalcolabili benefici al settore produttivo domestico[13]. Lo stesso discorso vale per un'organizzazione internazionale quale l'Unione europea che, dal canto suo, non è stata risparmiata da questa ondata di protezionismo che ha reso la *data localization* il principale attore non protagonista delle normative concernenti la gestione dei dati. Invero, più di uno studio sulle legislazioni vigenti nei singoli Stati membri dell'Unione ha dimostrato che, anche nel nostro continente, l'aumento del valore dell'informazione è stato accompagnato da un clima di sfiducia nelle normative e, soprattutto, nei sistemi di sicurezza degli altri Paesi membri, sfociando in poco tempo nell'emanazione di una serie di obblighi giuridici atti ad internalizzare il trattamento nella misura più ampia possibile[14].

Resosi conto di questa preoccupante tendenza, con l'inizio della seconda decade di questo secolo, il legislatore europeo ha deciso di prendere una posizione netta al riguardo, invertendo la rotta nel tentativo di ristabilire un clima di fiducia reciproca in tutto il continente. Con queste premesse nasce la strategia per la creazione del "Mercato Unico Digitale", concepito nelle intenzioni delle istituzioni europee come un passo imprescindibile affinché il mercato interno possa continuare a funzionare nell'era della digitalizzazione[15]. Oggi è, difatti, impossibile condurre un'attività economica con caratteri transfrontalieri senza far fronte a tutte le questioni connesse al tema

del trasferimento delle informazioni: i dati devono necessariamente muoversi assieme al bene al quale ineriscono, pertanto, in un mercato in cui gli ostacoli allo spostamento di persone, merci, capitali e servizi sono stati abbattuti, è chiaro che l'incentivo alla libera circolazione delle informazioni si manifesta come un passaggio irrinunciabile[16].

Tra l'altro, riuscire nell'intento di trasformare simili iniziative in disposizioni normative efficaci ed innovative rappresenta uno dei pochi ambiti in cui il vecchio continente può ancora imporsi quale capofila: se l'arretratezza tecnologica nei confronti dei giganti del tech che hanno le loro sedi nel Nord America e nell'Asia orientale non sembra potersi recuperare nel breve termine[17], agire per rendere il mercato continentale più appetibile rimane un dovere dell'Unione europea[18]. Segnatamente, i primi passi mossi dagli organismi dell'Unione verso la soppressione delle barriere virtuali alla libera circolazione, in favore di un incremento nell'utilizzo transfrontaliero delle informazioni, risalgono al 2011, quando la Commissione europea riconosce che le precedenti normative in materia di armonizzazione e di incentivo all'apertura nell'utilizzo dei dati nel settore pubblico – in particolare la Direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico – non hanno sortito gli effetti sperati e che, di fatto, le barriere allo scambio di informazioni pubbliche costituiscono ancora un peso per l'economia continentale[19]. Tuttavia, dati i tempi non ancora maturi per una discussione profonda come quella odierna, soprattutto per quanto riguarda la distinzione tra dato personale e non personale[20], il documento circoscrive i suoi riferimenti ai dati pubblici, salvo qualche sporadico accenno alla tutela della vita privata ed alla protezione dei dati personali[21].

Dopo un'ulteriore comunicazione del luglio 2014 in cui viene evidenziato il problema degli ostacoli alla libera circolazione dei dati ed il loro effetto frenante nei confronti dello sviluppo del *cloud computing* e dello sfruttamento dei big data[22], i documenti istituzionali del biennio 2017-2018 si focalizzano quasi esclusivamente sugli sforzi necessari alla creazione del mercato unico digitale. Secondo la visione europea, lo sviluppo di tutte le tecnologie basate sullo scambio di informazioni – dal *cloud computing*, all'*Internet of Things*, dalla *data analysis*, all'intelligenza artificiale – sono in grado di crescere e prosperare all'interno dell'economia continentale grazie a due pilastri fondamentali. Da un lato, la protezione dei dati personali, la quale, una volta aggiornata e consolidatasi nell'ordinamento europeo a tutti i livelli[23], promette di mantenere l'essere umano come centro gravitazionale attorno al quale si sviluppa la tecnologia, e non viceversa. Dall'altro lato, invece, si trova la libera circolazione dei dati, sia personali che non, la quale, accompagnata da una (non ancora del tutto) aggiornata disciplina riguardante l'interoperabilità e l'accesso alle informazioni, costituirà un incentivo senza eguali al progresso dell'economia europea.

Tuttavia, ciò che distingue l'ordinamento europeo dai regimi giuridici dei Paesi tecnologicamente più avanzati, è proprio la preponderanza che il primo dei due pilastri, la protezione dei dati personali, assume nei confronti della libera circolazione delle informazioni. Prendendo come termine di paragone due fra i Paesi leader dell'attuale panorama mondiale, negli Stati Uniti la regolamentazione riguardante le informazioni relative alle persone fisiche viene ancora percepita in un'ottica perlopiù consumeristica, con la conseguenza che l'individuo riesce ad ottenere protezione proprio in quanto consumatore, ma non in quanto persona che gode di un diritto fondamentale alla protezione dei propri dati[24]. Una impostazione altrettanto differente è invece quella riguardante la Repubblica popolare cinese, dove, in un certo senso, traspare una duplice concezione: se, per un verso, l'ordinamento cinese sembra si stia avvicinando a quello europeo nell'ambito delle relazioni fra privati, per altro verso, il precedente approccio centralizzato continua a caratterizzare la disciplina nei rapporti verticali fra individuo e governo, secondo un sistema autoritario e gerarchico che pone al vertice la sicurezza dello Stato[25].

Nell'ordinamento europeo, invece, il ruolo cardine attribuito alla persona fisica ed ai suoi diritti fondamentali rappresenta il principale motivo per cui l'impianto normativo dedicato alle altre dimensioni del *data law*, soprattutto, quella economica, si sia sviluppato in un secondo momento o, quantomeno, sia stato ipotizzato come sussidiario. Infatti, è dopo l'approvazione del Regolamento generale sulla protezione dei dati personali (GDPR)[26], precisamente nella Comunicazione sulla costruzione di un'economia dei dati europea del 2017, che è stata concepita l'idea di un regolamento specificamente dedicato ai dati a carattere non personale[27]. Effettivamente, dal testo emerge la ormai raggiunta consapevolezza che per lo sviluppo di un'economia sana e stabile non è sufficiente la sola tutela dell'individuo, poiché si rivela fondamentale anche mettere le imprese e le pubbliche amministrazioni in una posizione che dia loro la possibilità di essere promotrici di un nuovo modello economico-sociale[28]. Pertanto, la Commissione sottolinea quanto sia importante un approccio organico alla materia e chiarisce espressamente che il principio della libera circolazione dei dati all'interno dell'Unione, inteso quale corollario imprescindibi-

le delle altre libertà riconosciute nel mercato unico europeo, non riguarda solo i dati personali – come avviene nel GDPR – ma interessa tutte le tipologie di informazioni[29]. Tuttavia, subito dopo questa statuizione che potremmo definire pionieristica, interviene una ulteriore precisazione volta a rimarcare la differenza insita in quei regimi giuridici dei dati che attuano il medesimo principio di libera circolazione: mentre le norme concernenti il flusso dei dati possono essere il risultato di trattative con Paesi terzi, quelle relative alla protezione dei dati personali hanno uno status diverso, in quanto, godendo del rango di diritti fondamentali, non possono essere oggetto di negoziazione[30].

Un ulteriore documento finalizzato alla costruzione delle fondamenta del mercato unico digitale, in cui l'eterogeneità del regime giuridico europeo in materia di circolazione dei dati si avverte con maggiore evidenza, è la Comunicazione "Verso uno spazio europeo comune dei dati". In tal caso, lo scopo principale della Commissione risiede nella proposizione del cosiddetto *data package*, ossia di un insieme di tre provvedimenti che, in aggiunta alla normativa sulla protezione dei dati personali appena entrata in vigore ed al regolamento sulla circolazione dei dati non personali – all'epoca non ancora definitivamente approvato –, mira a creare "uno spazio comune dei dati nell'UE, un'area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati"[31].

La proposta della Commissione sfocia nell'adozione di tre documenti diversi che, nonostante non si traducano tutti in strumenti di *hard law*, di fatto predispongono o incentivano la creazione di regole differenti per i dati a seconda del settore in cui essi vengono trattati[32]. Se il primo strumento, ossia la direttiva relativa al riutilizzo dell'informazione nel settore pubblico, fa riferimento ad un ampliamento della politica di messa a disposizione dei dati definiti come "pubblici"[33], il secondo consiste in una Raccomandazione volta ad incentivare il regime di *open access* per i dati raccolti e trattati nell'ambito della ricerca scientifica[34]. Il terzo provvedimento, infine, riguarda gli orientamenti sulla condivisione dei dati nel settore privato, tramite i quali la Commissione si offre quale promotrice di principi, accordi e regole a cui gli operatori privati dovrebbero fare ricorso al fine di trasformare il mercato europeo in un grande *hub* di informazioni, da cui tutti potrebbero trarre beneficio[35]. Ciò che accomuna i tre provvedimenti è l'idea di una politica, o meglio, di una cultura di condivisione dei dati che non si limiti semplicemente al settore pubblico – già in parte destinatario di un'apposita direttiva – ma che riguardi anche il settore privato nei rapporti tra imprese e nei rapporti tra imprese ed enti pubblici. Peraltro, nonostante l'intenzione fosse quella di incentivare lo spostamento delle informazioni all'interno del territorio continentale nella misura più ampia possibile, è evidente che la vasta gamma di strumenti regolatori messi in campo dalle istituzioni europee rischia di produrre una settorializzazione e stratificazione normativa in grado di compromettere la libera circolazione[36].

3. La circolazione dei dati personali

3.1. All'interno dell'Unione europea

Come detto, la disciplina riguardante il flusso dei dati personali in Europa è frutto dell'evoluzione normativa che negli anni recenti ha elevato la tutela dell'individuo con riferimento al trattamento delle sue informazioni al rango di diritto fondamentale. Conseguentemente, l'impianto normativo è concepito in maniera tale che la tutela giuridica continentale rimanga il più a lungo possibile ancorata all'informazione, continuando a seguirla in ogni suo spostamento, come una garanzia che non può essere scissa dal bene al quale si accompagna[37]. Questo principio pervade l'intera normativa e, infatti, ha rappresentato uno dei capisaldi attorno ai quali sono state plasmate le disposizioni in materia di circolazione dei dati personali, sia dal punto di vista interno, ossia limitato al flusso intra-europeo, sia dal punto di vista esterno, quando i dati lasciano l'Unione.

Per quanto riguarda la circolazione tra gli Stati membri, con l'impiego della fonte regolamentare in luogo della precedente direttiva, il legislatore europeo è riuscito ad uniformare le discipline nazionali, cosicché, almeno teoricamente, ogni regime giuridico conforme al GDPR deve assicurare lo stesso livello di tutela[38]. Pertanto, alla luce della forte spinta verso l'armonizzazione in materia di protezione dei dati, l'articolo 1, paragrafo 3 del GDPR stabilisce che i singoli Stati membri non possono più lamentare una lacuna nella protezione di tali dati come motivo alla base dell'imposizione di un divieto di trasferimento al di fuori dei propri confini[39]. Invero, nonostante anche la precedente direttiva esordisse con parole simili, la mancata armonizzazione dovuta all'impiego di una fonte normativa "più debole" non era di fatto riuscita a limitare la propagazione degli obblighi di localizzazione dettati da motivi attinenti alla tutela della privacy delle persone fisiche. Anzi, proprio gli ultimi anni di vigenza della precedente direttiva sono stati testimoni di una proliferazione di restrizioni senza precedenti, non solo a causa dell'avvento della digitalizzazione, ma anche perché la promessa di un

elevato livello di protezione dei dati veniva utilizzata come giustificazione di tali misure[40].

Ad ogni modo, nonostante la libera circolazione non venga espressamente annoverata tra i principi fondamentali del GDPR, una chiara affermazione in tal senso proviene direttamente dalla Commissione europea la quale, nell'intento di allargarne l'applicazione anche ai casi in cui agli Stati membri è consentito disciplinare materie specifiche, afferma che questi "dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati"[41].

Tuttavia, se il Regolamento generale sulla protezione dei dati personali rappresenta un apparato giuridico che, oltre che tutelare l'individuo, è funzionale al contrasto dell'insorgenza degli obblighi di *data localization*, è opportuno rammentare che i mezzi attraverso i quali gli Stati membri sono in grado di introdurre nuove restrizioni, o mantenere quelle già esistenti, non ricadono tutti nell'ambito di applicazione del GDPR[42]. Mentre la protezione della privacy degli individui non può più fungere da scudo della localizzazione, i singoli Paesi possono ancora fare affidamento sulle deroghe previste da altre fonti settoriali del diritto europeo riguardanti la gestione dei dati[43], le quali dovranno comunque superare il vaglio relativo alla loro compatibilità con quanto stabilito dal diritto dell'Unione in materia di libertà fondamentali[44].

A tal proposito, non ci si può esimere dal sottolineare ancora una volta come la moltitudine di fonti normative europee, nel tentativo di regolamentare dettagliatamente la gestione dei dati, non faccia altro che offrire ulteriori opportunità per l'introduzione di impedimenti al libero flusso delle informazioni.

3.2. Al di fuori dell'Unione europea

Un discorso diverso vale, invece, se si rivolge lo sguardo alle modalità con cui l'Unione europea disciplina la circolazione dei dati al di fuori dei propri confini, poiché è lo stesso ordinamento giuridico continentale a trasformarsi in un parziale obbligo di localizzazione dei dati personali.

Il meccanismo di trasferimento di informazioni personali verso Paesi terzi o organizzazioni internazionali muove dalla precedente impostazione sancita dalla Direttive 95/46/CE, riadattandola al nuovo contesto digitalizzato in cui si trova ad operare e, soprattutto, cristallizzando le regole di origine giurisprudenziale elaborate dalla Corte di giustizia dell'Unione nella vigenza della normativa ormai abrogata[45]. Pertanto, affinché i dati personali possano lasciare il territorio europeo, gli articoli 44 e seguenti del GDPR predispongono una serie di condizioni in assenza delle quali il trasferimento non può avere luogo. Dunque, nonostante il legislatore abbia predisposto un ampio ventaglio di possibilità di trasferimento capaci di adeguarsi al tipo di situazione in cui versa il titolare del trattamento, stando alla definizione generale di *data localization*, anche l'ordinamento giuridico europeo rientra a pieno titolo nel novero di quelle misure atte a limitare la libera circolazione[46].

Il ragionamento alla base del divieto di imporre obblighi di localizzazione all'interno dell'Unione, viene in questo caso impiegato *a contrario* proprio per condizionare il trasferimento verso l'esterno: dal momento in cui la tutela dei dati personali è ben lontana dal poter essere considerata omogenea a livello globale, l'Unione europea ha deciso di introdurre un meccanismo che sia in grado, quantomeno nelle intenzioni, di agganciare al dato la tutela europea, anche quando questo esce dall'ordinamento giuridico di origine[47]. Se da un lato, le norme europee appaiono come un garanzia imprescindibile nel panorama globale, dall'altro lato, non sono mancate insinuazioni volte a sollevare dubbi sul vero scopo dell'Unione nel predisporre un meccanismo di trasferimento così dettagliato. Non potendo essere alla pari di altre realtà dal punto di vista dello sviluppo tecnologico[48], sembra che l'Unione stia cercando di recuperare terreno sotto l'aspetto della disciplina giuridica, attraverso una applicazione extraterritoriale delle proprie regole[49], le quali, è bene ricordarlo, devono essere osservate, non solo la prima volta che i dati abbandonano l'Europa, ma anche per i trasferimenti successivi[50].

Entrando nel dettaglio, si nota sin da subito come il Regolamento generale racchiuda una serie di regole in cui il flusso internazionale dei dati è percepito come un "elemento strutturale"[51] della normativa e non più, come accadeva nella Direttiva – in vigore in un momento storico in cui lo spostamento delle informazioni tra Stati non aveva la rilevanza che ha oggi – come circostanza episodica annoverabile fra le ipotesi delle mere eccezioni. Dunque, la disciplina che governa il meccanismo di trasferimento esordisce con il principio in ragione del quale i dati possono lasciare il territorio europeo solamente se rispettano le condizioni del capo V. Lungi dal prescrivere un divieto generale come le misure restrittive più rigide, la consapevolezza raggiunta dal GDPR in merito alla essenzialità del flusso internazionale dei dati lo colloca nel complesso degli obblighi di localizzazione condizionali più tenui fra quelli attualmente in vigore[52].

A conferma di ciò, è possibile constatare che se la decisione di adeguatezza, di cui all'articolo 45[53], rimane il metodo principe per il trasferimento come avveniva in precedenza[54], ora questo stesso stru-

mento viene potenziato poiché tanto il diritto europeo quanto quello nazionale non possono fissare limiti al trasferimento extra-europeo nei confronti di quei Paesi o organizzazioni internazionali il cui ordinamento giuridico è stato riconosciuto come adeguato[55]. Tale previsione si inserisce nel disegno generale promosso dal legislatore europeo verso quella che sembra essere una maggiore apertura del continente, con lo scopo di rafforzare le relazioni con altri Paesi, senza però sacrificare la tutela dell'individuo[56].

Un ulteriore aggiornamento concerne la nuova impostazione assunta dal GDPR in materia di deroghe. Se prima tutto ciò che ricadeva fuori dalla decisione di adeguatezza era classificato come deroga, oggi questa qualifica spetta solamente alle ipotesi specifiche – e più numerose rispetto al passato –[57] elencate nell'articolo 49[58]. Ciononostante, la predisposizione di un sistema derogatorio apparentemente a maglie più larghe, non si traduce in un lasciapassare volto ad eludere le disposizioni in materia di protezione di dati: il Comitato europeo per la protezione dei dati è intervenuto sul punto con delle apposite linee guida, insistendo sul fatto che l'interpretazione delle disposizioni all'articolo 49 deve essere la più restrittiva possibile[59].

Infine, sulla base della stessa logica innovativa sono state aggiornate le garanzie adeguate, ossia quelle misure per mezzo delle quali è possibile trasferire i dati personali verso un Paese terzo il cui ordinamento giuridico non è stato valutato come adeguato da parte della Commissione europea. Il sistema in vigore, oltre a risultare più centralizzato rispetto al passato grazie ai maggiori poteri di controllo preventivo ed autorizzatorio concessi agli attori istituzionali, dimostra ancora una volta la presa di coscienza da parte del Regolamento del fatto che il movimento dei dati da un continente all'altro sia diventato un elemento essenziale dell'economia moderna. Il GDPR riesce a bilanciare la tutela dell'individuo con la circolazione dei dati personali tramite la responsabilizzazione dei soggetti coinvolti, ossia titolari e responsabili del trattamento, i quali, siano essi mittenti o riceventi, devono definire misure negoziali o paranegoziali al fine di sopperire alle lacune del sistema giuridico applicabile[60]. Oltre all'impiego di clausole contrattuali tipo, codici di condotta, meccanismi di certificazione o altri strumenti vincolanti, una delle principali novità risiede nell'introduzione delle "norme vincolanti d'impresa" (*Binding Corporate Rules*, o BCRs)[61]. Mentre nel testo della Direttiva non erano affatto prese in considerazione[62], queste disposizioni sono state concepite al preciso scopo di favorire lo scambio di informazioni sia nei gruppi imprenditoriali che nei "gruppi di imprese che svolgono un'attività comune"[63], di fatto prevenendo la formazione di barriere alla libera circolazione di informazioni che ostacolerebbero non poco l'attività commerciale del gruppo. L'inserimento delle BCRs e l'aggiunta di un articolo a sé stante nel regolamento segnano una presa di posizione forte da parte dell'Unione europea poiché, dalla totale assenza nella normativa precedente, sono ora divenute un *unicum* nel panorama del trasferimento extra-europeo dei dati personali, differente da tutte le altre garanzie[64].

Ad ogni modo, il fatto che l'ordinamento giuridico europeo risulti essere una normativa moderna, attenta alle esigenze delle imprese che conducono attività a carattere transfrontaliero e più permissivo rispetto ad altri sistemi giuridici, non è sufficiente a precluderne la qualificazione di regime giuridico di *data localization*[65]. Oltretutto, questa situazione sembra destinata a permanere ancora a lungo, giacché, se la motivazione alla base di questa restrizione risiede nella tutela della privacy degli individui che in altri ordinamenti potrebbe risultare non adeguatamente salvaguardata, l'eventuale soppressione delle condizioni restrittive presupporrebbe il raggiungimento di un livello di armonizzazione globale che, ad oggi, sembra lontano[66]. Invero, dal momento che numerosi Paesi stanno virando verso un'impostazione giuridica in materia di tutela di dati e di localizzazione degli stessi non necessariamente simile a quella del vecchio continente, si può presumere che negli anni avvenire, anziché ad una omogeneizzazione della normativa, assisteremo all'acuirsi dell'arroccamento all'interno delle proprie fortezze informatiche da parte di Stati gelosi del proprio patrimonio digitale.

4. La circolazione dei dati non personali

Nella mente del legislatore europeo, il Regolamento relativo ad un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (RDNP)[67] nasce come strumento diretto a colmare le lacune insorte in seguito all'approvazione del GDPR, il quale, circoscrivendo il suo ambito di applicazione alla categoria dei dati personali, aveva lasciato senza copertura altre tipologie di informazione e i relativi obblighi di localizzazione[68]. Così, al termine di un iter durato all'incirca un anno, precisamente nel 2018, il Regolamento sulla libera circolazione dei dati non personali è stato approvato e a partire dal 28 maggio 2019 trova applicazione nel territorio europeo.

Prima di procedere alla valutazione dell'impatto che la nuova disciplina ha avuto ed avrà con riguardo alla circolazione delle informazioni, è doveroso fare due osservazioni preliminari. La prima è volta a for-

nire una definizione della nuova categoria del dato non personale. A tal proposito, non sembra essere sufficientemente esaustiva la sola lettura dell'articolo 3 del RDNP che, nel primo punto, afferma che i dati non personali sono quelli "diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679"[69]. Pertanto, consapevole delle problematicità giuridiche che di regola si accompagnano alle definizioni di carattere negativo, l'articolo 8, paragrafo 3 del RDNP, ha attribuito alla Commissione europea il compito di formulare ulteriori "orientamenti informativi" atti a specificare il regolamento. Conseguentemente, le linee guida pubblicate a maggio dello scorso anno in ossequio a suddetta disposizione si sono rivelate estremamente opportune, in quanto contenenti una definizione più puntuale della nozione di dato non personale che, invece, non è presente nel testo del Regolamento. Pertanto, grazie al lavoro della Commissione, è ora possibile affermare che la categoria "dato non personale" è costituita sia dalle informazioni che sin dall'origine non si riferivano a una persona fisica identificata o identificabile[70], sia dalle informazioni che, pur inizialmente personali, sono state anonimizzate in un secondo momento.

Peraltro, è pur sempre doveroso osservare che la scelta di demandare (quantomeno in parte) la definizione di questa nuova fattispecie ad un atto il cui valore giuridico all'interno dell'ordinamento europeo non può di certo essere equiparato a quello delle fonti regolamentari, potrebbe comportare seri problemi di coordinamento con altre normative continentali e, soprattutto, potrebbe mettere a rischio la certezza e l'applicazione uniforme del diritto nell'Unione europea. Le linee guida della Commissione, difatti, nonostante offrano un punto di vista autorevole per l'interpretazione del diritto europeo e, in quanto tali, risultino funzionali a risolvere alcuni problemi in chiave applicativa del RDNP, rimangono pur sempre prive della forza di legge che contraddistingue le disposizioni contenute nel regolamento[71]. L'indeterminatezza riguardante la questione definitoria corre il rischio di minare la coerenza di qualificazione del dato fra gli ordinamenti giuridici degli Stati membri, specialmente in quegli ambiti in cui ciò è reso più difficoltoso sia dalle potenzialità di re-identificazione offerte dagli sviluppi tecnologici[72], sia dai margini di discrezionalità lasciati ai singoli ordinamenti nazionali, come avviene nel caso dei dati relativi alle persone fisiche decedute[73]. Naturalmente, la poca chiarezza che attiene alla disposizione cardine della nuova disciplina non potrà che avere ripercussioni negative sulla distinzione, ben lungi dall'essere pacifica[74], tra dato personale e non personale e sull'applicazione dei due regolamenti europei[75].

La seconda osservazione, invece, mira a sottolineare la profonda differenza che intercorre tra il Regolamento generale sui dati personali ed il RDNP per quanto concerne la disciplina della circolazione delle rispettive categorie di informazioni. Se, a differenza di quanto fatto dal GDPR nei confronti dei dati personali, il RDNP è principalmente focalizzato sul tema della circolazione e dell'accesso delle autorità amministrative in una dimensione prettamente interna, la sorte che spetta ai dati non personali – che sfuggono all'applicazione del meccanismo condizionale previsto dagli articoli 44 e seguenti del GDPR – nell'ipotesi in cui essi vengano destinati verso Paesi terzi non sembra essere stata presa in debita considerazione[76]. Pertanto, se da un lato, salvo l'unica eccezione relativa alla pubblica sicurezza che si vedrà in seguito, il regolamento non sembra contenere disposizioni di *data localization*, dall'altro, la mancanza di riferimenti alla dimensione extraeuropea potrebbe incoraggiare lo spostamento di informazioni di inestimabile valore per lo sviluppo delle nuove tecnologie in ordinamenti giuridici che rispondono a regole diverse, incentivando, pertanto, lo sfruttamento di questi dati solamente all'estero, dove l'Unione europea non potrebbe né controllarli né trarne alcun beneficio[77].

Rivolgendo ora l'attenzione a quanto avviene all'interno del territorio continentale, è possibile osservare che il legislatore europeo ha deciso di incentivare la libera circolazione concentrando i propri sforzi, sia verso il settore pubblico, con l'abbattimento degli obblighi di localizzazione derivanti da legislazioni o pratiche amministrative in vigore negli Stati membri[78], sia verso il settore privato, tramite l'incoraggiamento della portabilità delle medesime informazioni nell'ambito delle attività degli utenti professionali[79], in maniera tale da prevenire le pratiche di *vendor lock-in* nemiche del mercato unico[80].

4.1. Il divieto degli obblighi di localizzazione

Il primo scopo che il RDNP intende conseguire è quello di eliminare le restrizioni ingiustificate alla libera circolazione dei dati non personali, considerate dalla Commissione europea il più grande ostacolo allo sviluppo dell'economia dei dati nell'Unione[81]. In virtù di ciò, la norma centrale del regolamento è l'articolo 4, paragrafo 1, il quale vieta agli Stati membri l'introduzione e il mantenimento di obblighi di localizzazione dei dati quando non giustificati da motivi di pubblica sicurezza[82]. Ai fini del Regolamento, sono identificati quali obblighi di localizzazione le disposizioni di legge, gli orientamenti o le pratiche amministrative che, direttamente o indirettamente,

impongono l'elaborazione o la conservazione dei dati limitatamente ad una determinata area geografica[83]. In particolare, i documenti degli organi europei fanno spesso riferimento alle richieste delle autorità di controllo di archiviare localmente i propri dati, alle regole del segreto professionale che prediligono il trattamento a livello locale, alle linee guida amministrative che dispongono lo stesso principio relativamente ai dati gestiti da enti pubblici e, non da ultimo, alle norme di settore che impongono l'utilizzo di dispositivi omologati in un determinato Stato membro[84].

L'identificazione di simili restrizioni risulta molto più complessa di quanto possa apparire a prima vista. Uno studio di particolare interesse, eseguito anteriormente all'adozione definitiva del Regolamento, tende a distinguere tra due diverse categorie[85]. *In primis*, ci sono le cosiddette "barriere dirette", individuabili in maniera più agevole, le quali includono tutte le misure normative che stabiliscono espressamente dove conservare – o non conservare – i dati oppure che contengono obblighi tali per cui il loro rispetto può essere garantito solo tramite la conservazione in un determinato territorio[86]. Più ardue da riconoscere sono, invece, le "barriere indirette". Queste comprendono quelle norme la cui interpretazione può ragionevolmente limitare la scelta di chi gestisce i dati per quanto riguarda il luogo di archiviazione ed il libero flusso. La maggiore difficoltà deriva dal fatto che l'obbligatorietà della restrizione, essendo strettamente correlata all'interpretazione, potrebbe non essere uniformemente intesa[87].

La categoria delle barriere indirette, nonostante i suoi confini piuttosto sfumati, non può essere affatto sottovalutata, dal momento in cui al suo interno si cela la maggioranza degli ostacoli alla libera circolazione dei dati non personali: lo studio citato giunge alla conclusione che, delle quaranta barriere totali rinvenute al termine dell'analisi, trenta rientrano proprio in questa categoria più "sibillina"[88]. In realtà, alla luce delle ipotesi analizzate[89], questo squilibrio non desta troppo stupore: la circostanza che i dati debbano, da un lato, essere obbligatoriamente resi disponibili ai titolari del trattamento o alle autorità di vigilanza, mentre, dall'altro, non possano essere resi noti a terze parti, unita ai troppo spesso frequenti obblighi di autorizzazione prescritti per poter utilizzare una determinata struttura di archiviazione o un determinato responsabile del trattamento[90], possono verosimilmente spingere chi accumula queste informazioni a preferire una soluzione domestica – e magari più costosa in termini di conservazione – in luogo di una più funzionale alla propria impresa, ma che potrebbe attirare attenzioni indesiderate da parte delle autorità di controllo.

Peraltro, la questione degli obblighi di localizzazione permette di individuare una significativa differenza del Regolamento sui dati non personali rispetto al GDPR. Mentre il regolamento riguardante i dati personali concentra la sua attenzione, in primo luogo, sui soggetti che intervengono nella filiera del trattamento dei dati – il titolare ed il responsabile del trattamento – stabilendo gli obblighi da rispettare al fine di assicurare una tutela efficiente al *data subject*, il RDNP dedica la sua norma cardine agli Stati membri. D'altronde, non potrebbe essere diversamente giacché, se per il GDPR l'obiettivo (primario) è quello di tutelare un diritto fondamentale dell'individuo, il secondo regolamento si inserisce, invece, in quella serie di strumenti che, incentivando la circolazione, mirano a rafforzare il mercato unico[91]. Ad ulteriore conferma del ruolo di destinatari principali della disciplina ricoperto dai Paesi membri, il testo del Regolamento tiene a precisare che la normativa non è volta né a ridurre le facoltà di scelta delle imprese in relazione alla localizzazione dei dati, le quali rimangono comunque libere di optare per una soluzione domestica[92], né ad imporre l'esternalizzazione dei servizi da parte degli enti pubblici quando sussistono esigenze che li spingono a preferire l'autofornitura[93].

Come anticipato, la presa di posizione dell'Unione europea nei confronti della *data localization* nell'ambito della circolazione dei dati non personali scaturisce dal preoccupante aumento di misure restrittive verificatosi negli ultimi anni, spesso dettato dalla convinzione che la conservazione e l'analisi dei dati all'interno dei confini nazionali siano sinonimo di sicurezza oppure che facilitino l'accesso e la sorveglianza da parte delle autorità. In aggiunta, alcune limitazioni sono state imposte al preciso scopo di sfavorire i fornitori di servizi stranieri o multinazionali rispetto a quelli nazionali[94]. Stando alle stime prettamente economiche presentate dalla Commissione europea, la drastica diminuzione di queste restrizioni voluta dal nuovo regolamento permetterebbe all'economia dei dati di crescere fino a 739 miliardi di euro entro il 2020[95]. Oltretutto, secondo uno studio dello *European Centre for International Political Economy* (ECIPE), l'effetto sarà più che positivo per il mercato, poiché, beneficiando le industrie di costi minori legati alla maggiore flessibilità nella gestione dei propri dati, il PIL potrebbe crescere di circa 8 miliardi di euro l'anno[96]. Pertanto, la Commissione, al fine di cogliere le opportunità offerte dall'economia dei dati, ha ritenuto necessario garantire il libero flusso delle informazioni stabilendo il medesimo principio di libera circolazione, ma garantendolo tramite due fonti diverse, il GDPR, per il versante

dei dati personali ed il RDNP, per quello dei dati non personali[97]. Sebbene offrano un quadro all'apparenza nitido, le valutazioni della Commissione si focalizzano quasi esclusivamente sull'aspetto economico connesso all'aumento delle misure restrittive alla circolazione dei dati, senza tuttavia approfondire ulteriori profili che meritano di essere presi in considerazione. In tal senso, alcune delle ultime iniziative promosse tanto a livello europeo[98], quanto a livello nazionale[99], non sembrano avere come obiettivo una riappropriazione del bene "dato" in chiave monopolistica e con l'intento di escluderne gli altri dal *management* ma, al contrario, tentano con non poche difficoltà di riconquistare il terreno perduto dagli ordinamenti giuridici nazionali e sovranazionali in un ambito, quello della gestione dei dati a valenza strategica, in cui la posizione centrale un tempo ricoperta è stata fortemente ridimensionata dall'entrata in campo dei servizi offerti dagli OTT[100]. Pertanto, se per un verso, il gravame economico derivante da simili politiche è innegabile, per altro verso, la questione della *data localization* potrebbe essere riletta come un timido tentativo attuato dalle istituzioni del vecchio continente di stabilire un regime concorrenziale con riguardo al trattamento dei dati, attraverso la realizzazione di infrastrutture proprie che siano in grado di operare parallelamente a quelle ben più avanzate dei giganti del tech.

4.1.1. La sicurezza pubblica come unica eccezione

L'articolo 4 del Regolamento sulla libera circolazione dei dati non personali prevede come unica eccezione al divieto di imporre obblighi di localizzazione la sicurezza pubblica. Al fine di evitare l'insorgere o il permanere di discipline non fondate su tale base legittima, grava sugli Stati membri il dovere di procedere alla disamina di tutte le norme che impongono un obbligo di localizzazione per poi abrogare quelle non conformi al Regolamento. Tuttavia, nel caso in cui ritengano necessario il mantenimento di alcune misure restrittive, proprio perché fondate su motivi di pubblica sicurezza, devono darne comunicazione alla Commissione europea allegando la relativa giustificazione[101]. Per contro, alla Commissione è riconosciuta la facoltà di presentare osservazioni qualora ritenga opportuno che tali disposizioni debbano essere modificate o addirittura abrogate, in quanto non confacenti ai principi sanciti dal diritto comunitario[102] o dalla giurisprudenza della Corte di giustizia dell'Unione[103].

Il considerando n. 19 del RDNP agevola l'interpretazione del significato di sicurezza pubblica. Innanzitutto, il riferimento alla sicurezza sia interna che esterna permette di trattenere tutte le informazioni potenzialmente utili ai fini di prevenzione di attacchi provenienti da Paesi terzi, di fatto legittimando la conservazione di dati relativi a contesti non nazionali o non europei. Appare in tal caso evidente il legame con la speciale disciplina antiterrorismo diffusasi in tutto il continente a seguito degli attacchi terroristici degli anni recenti. Come evidenziato dalla dottrina, il timore di essere vittime di simili aggressioni ha scatenato la proliferazione di normative *ad hoc* che hanno eroso alcuni diritti fondamentali degli individui – soprattutto il diritto alla protezione dei dati personali – in nome della pubblica sicurezza[104]. *A fortiori*, un simile atteggiamento potrebbe contraddistinguere la regolamentazione dei dati non personali: scevro da rischi di lesione diretta ai diritti fondamentali della persona fisica, lo Stato tenterà di trattenere nelle proprie banche dati quante più informazioni possibili, legittimato dall'interesse alla difesa delle "questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati"[105].

Nel prosieguo, la normativa sembra ampliare di molto il novero di interessi legittimanti una deroga. Difatti, nell'esigere una minaccia "reale e sufficientemente grave ad uno degli interessi fondamentali della società", vengono espressamente riportati "il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari".

In questa definizione a prima vista dettagliata, potrebbero nascondersi non poche insidie interpretative: basti pensare al concetto di servizio pubblico essenziale, il quale, non godendo di una definizione uniforme a livello continentale[106], rischia di creare una disparità di trattamento tra i diversi Stati membri. Altrettante incertezze accompagnano le nozioni di incolumità pubblica e interessi militari. Se la prima può potenzialmente impedire la circolazione di numerose informazioni relative alla salute dei cittadini – già oggetto di significative barriere indirette secondo lo studio sopra citato –[107], gli interessi militari, a loro volta, tolgono dalla circolazione, non solo le informazioni *latu sensu* strategiche, ma anche la maggior parte dei dati relativi alla produzione di materiale utilizzato dalle forze armate, detenuti dalle industrie belliche.

Se questi sono i presupposti, è probabile che gli Stati membri, desiderosi di mantenere le informazioni più delicate nel territorio in cui possono esercitare un potere "diretto", daranno un'interpretazione

estensiva al concetto di sicurezza pubblica, al preciso scopo di limitare la fuoriuscita dei dati nella misura più ampia possibile. A tal riguardo, sono condivisibili le perplessità espresse dal Comitato economico e sociale europeo (CESE) con riferimento alla imprecisione con cui viene delineata questa nozione ed alla mancanza di un "riferimento alle controversie o alle modalità per verificare in che modo gli Stati membri rispetteranno i criteri della pubblica sicurezza, né ad eventuali sanzioni nei loro confronti, ove opportuno"[108].

Quanto detto assume particolare rilevanza a fronte del contesto in cui operano alcune agenzie governative, reso noto a seguito delle rivelazioni riguardanti la vicenda *Datagate*[109]. Questa esperienza ha dimostrato che ad essere interessati al possesso di dati non sono solamente le compagnie private, ma anche le agenzie di intelligence che, proprio al fine di garantire la sicurezza pubblica, si sono rese protagoniste di una raccolta massiva di informazioni mai vista nella storia[110]. È bene notare che, nonostante il dibattito manifestatosi in seno all'opinione pubblica a partire dal 2013 si sia concentrato sulla violazione della vita privata degli individui sottoposti a sorveglianza, le stesse osservazioni potrebbero essere svolte, *mutatis mutandis*, in relazione ai dati a carattere non personale. Ne è un esempio significativo il comprovato meccanismo in voga fra i funzionari degli organi inquirenti consistente nel chiedere accesso alle informazioni detenute da imprese private nel settore ICT. Richieste che nella maggior parte dei casi non trovano nessuna base giuridica riconosciuta dalla legge e che, solitamente, vengono assecondate per motivi di reverenza o per timore di ripercussioni negative[111].

In un certo senso, sussiste la possibilità che, grazie allo schermo della sicurezza pubblica, possa venire alla luce anche per i dati non personali una differenziazione già nota per quelli personali. Se il Regolamento generale assicura una disciplina giuridica parzialmente diversa – *rectius*, più stringente – per le cosiddette categorie particolari di dati[112], è plausibile che in futuro si andrà a delineare una distinzione simile anche per i dati non personali. Riprendendo la vecchia nomenclatura tanto cara al nostro legislatore[113], una sorta di dato non personale "sensibile", ossia un dato che per la sua connessione funzionale con l'interesse collettivo della sicurezza pubblica, giustifica un regime giuridico diverso, grazie al quale lo Stato può imporre all'ente che lo conserva, pubblico o privato che sia, un obbligo di localizzazione[114].

In ultima analisi, essendo ancora nella fase iniziale di vigenza del RDNP, l'ampiezza dell'area che il concetto di pubblica sicurezza andrà concretamente a ricoprire verrà definita dalla prassi degli Stati membri e, soprattutto, dall'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea, la quale, al fine di dare corpo alla nuova normativa, potrebbe ridurre la discrezionalità interpretativa riconosciuta dal regolamento.

4.2. Una nuova portabilità autoregolamentata

A seguito della risonanza che il diritto alla portabilità dei dati personali ha avuto con l'entrata in vigore del GDPR, anche per il Regolamento sui dati non personali viene sottolineato sin da subito l'impatto positivo che il libero trasferimento delle informazioni da un fornitore di servizi ad un altro, su richiesta dell'utilizzatore e senza costi eccessivi, potrebbe avere nei confronti della concorrenza nel mercato interno[115]. Inoltre, è lo stesso testo della nuova disciplina che effettua una comparazione fra il diritto già vigente nell'Unione – in particolare il GDPR – che garantisce una tutela solida al consumatore desideroso di cambiare il prestatore di servizi, e le lacune che, al contrario, riguardano la situazione in cui versano gli utenti professionali, i quali, sprovvisti di una simile protezione, spesso si trovano intrappolati a causa di pratiche di *vendor lock-in* che comportano oneri di mantenimento più alti ed, al contempo, danneggiano la competitività delle imprese[116].

Sfortunatamente, malgrado le premesse, per il particolare caso dei dati a carattere non personale il legislatore europeo ha deciso di intraprendere una strada diversa rispetto a quanto fatto nel 2016[117]: se alle persone fisiche è riconosciuto a livello normativo un vero e proprio diritto alla portabilità, gli utenti professionali possono solo fare affidamento sull'elaborazione di codici di condotta di autoregolamentazione che, benché supportata e controllata direttamente dalla Commissione, non riuscirà mai a garantire quella certezza del diritto e quella parità di condizioni che dovrebbero essere alla base dell'adozione di questo regolamento[118]. Oltretutto, è difficile comprendere perché ragioni quali la necessità di "mantenere il passo con la potenziale innovazione del mercato e tener conto dell'esperienza e delle competenze dei fornitori di servizi e degli utenti professionali di servizi di trattamento di dati"[119], possano giustificare una regolamentazione tramite codici di condotta in luogo di un vero e proprio diritto che sia in grado di bilanciare lo squilibrio di potere intercorrente tra tali utenti professionali, spesso piccole e medie imprese, e fornitori di servizi online, i quali con la digitalizzazione dei settori pubblico e privato, stanno velocemente trasformandosi negli attori più potenti del mercato[120].

La volontà del regolamento di distaccarsi in maniera netta dalla posizione adottata nel GDPR è di-

mostrata, prima che dalla predisposizione di una tutela giuridica più debole, anche dall'utilizzo di una terminologia differente: se l'individuo può fare affidamento sulla *portability* inglese o sulla *portabilité* francese, i codici di condotta devono essere orientati alla disciplina, rispettivamente, del *porting* o del *portage*[121]. Questa differenza terminologica deriva, probabilmente, dalla volontà di sottolineare in maniera chiara il tipo di relazione giuridica che viene presa in considerazione nei due testi. Il diritto alla portabilità di cui all'articolo 20 del GDPR fa riferimento ad una situazione giuridica in cui i due protagonisti sono, da un lato, l'interessato persona fisica e, dall'altro, colui che tratta le sue informazioni, il quale, di regola, incarna la figura del titolare del trattamento. Dunque, similmente a quanto si è visto nella tradizione statunitense[122], questo diritto si inserisce in un'ottica di tutela del consumatore nel rapporto con il fornitore del servizio[123]. Per i dati non personali, al contrario, l'articolo 6 circoscrive il suo riferimento non ad un utente generalmente inteso, bensì alla specifica categoria dell'utente professionale, il quale tratta i dati per fini connessi alla sua attività. Di conseguenza, il rapporto intercorrente tra l'utente professionale ed il fornitore di servizi di gestione di dati, più che in una dinamica B2C, può essere ricondotto nell'ambito business-to-business[124], similmente a quanto avviene nel caso di dati personali tra titolare del trattamento e responsabile del trattamento[125].

Ad avviso di chi scrive, la strategia che l'Unione europea ha deciso di perseguire appare discutibile. La necessità, più volte richiamata, del coinvolgimento delle PMI nel processo di elaborazione di questi codici di condotta non è uno strumento sufficientemente forte da dissuadere i dubbi che pervadono la preferenza per l'autoregolamentazione, soprattutto alla luce dell'attuale momento storico del mercato dei dati in cui poche grandi imprese stanno guadagnando capacità egemoniche. In questo frangente, l'Unione europea ha l'opportunità di distinguersi ancora una volta rispetto ad altre realtà giuridiche tramite una presa di posizione forte verso il riequilibrio di quella parità contrattuale che sembra essersi fortemente indebolita[126]. Proprio da tali esigenze sono di recente nate numerose istanze in ambito accademico volte a sollecitare un dibattito profondo sulla necessità di allargare la normativa a tutela del consumatore al fine di ricomprendere anche le piccole e medie imprese, così da scongiurare la formazione di posizioni dominanti che rischiano di alterare la libera concorrenza nel mercato europeo in modo irreversibile[127]. La prevenzione di pratiche simili potrebbe avvenire in maniera più efficace se solo il Regolamento fosse sceso più nel dettaglio, magari fissando a chiare lettere alcune delle norme inderogabili che i codici di condotta dovrebbero necessariamente includere oppure, come ha notato il CESE, definendo gli orientamenti da cui i meccanismi di autoregolamentazione dovrebbero muovere, non limitandosi al semplice richiamo alle migliori pratiche, agli obblighi informativi ed alle tabelle di marcia[128].

5. I punti deboli dell'impianto regolamentare europeo

Come si è avuto modo di vedere, l'ultimo decennio ha visto l'Unione europea assumere un ruolo centrale nel campo della regolamentazione del settore dei dati, attraverso una serie di iniziative che hanno gradualmente dato forma al mosaico del mercato europeo digitale. Tuttavia, le soluzioni di compromesso e le ampie lacune emerse al termine dell'iter legislativo che ha portato alla approvazione della disciplina del flusso dei dati non personali mostrano l'incompletezza di questo grande disegno[129].

In particolare, alcuni dei punti deboli della normativa in esame derivano da un contrasto che, benché preso in considerazione dal legislatore, non sembra essere stato risolto con una scelta adatta alle problematiche che titolari, responsabili del trattamento e gestori dei dati in genere si trovano ad affrontare quotidianamente. I regolamenti, le direttive e tutte le altre fonti, anche di *soft law*, adottate al fine di rendere l'economia dei dati alla portata di tutti sembrano essere lontane da una realtà dei fatti poliedrica ed interconnessa come quella odierna, con la conseguenza che quando differenti mondi entrano in contatto l'uno con l'altro tutto l'impianto normativo viene messo a dura prova.

Una chiara ipotesi in cui il Regolamento sui dati non personali sembra vacillare riguarda gli "insiemi di dati misti". Nonostante non vi sia una definizione esplicita nel Regolamento[130], sono considerati come tali quei dataset che sono composti sia da dati personali che da dati non personali. Il RDNP dedica a tale fattispecie il secondo paragrafo dell'articolo 2, il quale stabilisce che il Regolamento generale sulla protezione dei dati personali e quello sulla libera circolazione dei dati non personali si applicano alla rispettiva categoria di dati. Tuttavia – aggiunge la norma – quando tali insiemi sono "indissolubilmente legati"[131], il GDPR troverà applicazione nei confronti dell'intero dataset anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme[132], in ossequio alla costante logica della protezione prima della circolazione.

Il fenomeno in oggetto non sembra essere stato approfondito in maniera soddisfacente né dal Rego-

lamento, che, eccetto il riferimento alle valutazioni ed agli orientamenti della Commissione europea[133], gli dedica un solo paragrafo; né dalla Commissione stessa che nell'elaborazione di quelle linee guida che avrebbero dovuto semplificare il lavoro degli operatori del settore, si limita ad affermare che, in considerazione della diminuzione del valore derivante dalla eventuale separazione dell'insieme in dati personali e non personali, dell'assenza di una obbligo che imponga tale separazione e, soprattutto, del fatto che tali insiemi rappresentano la maggioranza dei dataset esistenti, il GDPR si applicherà, di regola, a tutti gli insiemi di dati misti[134].

In realtà, la vera falla del sistema da cui sembra provenire l'approccio, in un certo senso "sbrigativo", che traspare tanto dal testo del Regolamento quanto dalla guida della Commissione, può essere rinvenuta nel differente peso attribuito al concetto di rischio nei due regolamenti, il quale, creando un dislivello alla base delle normativa europea in materia di dati, contribuisce a rendere fragile l'intera struttura. Se il *risk-based approach* costituisce uno degli elementi qualificanti il Regolamento generale sui dati personali[135], la stessa cosa non può dirsi con riferimento alla disciplina dei dati non personali, dove la valutazione del rischio, che si rivelerebbe uno strumento assai utile per comprendere la natura del dato e per individuare le implicazioni che i dati non personali possono avere sull'insieme di dati misti, non viene presa in dovuta considerazione[136]. Difatti, la decisa accelerazione della digitalizzazione della società moderna ha messo in crisi la definizione stessa di dato personale, portando con sé innumerevoli difficoltà nell'individuazione della linea di confine tra carattere personale e non personale e causando non pochi disagi tanto ai titolari del trattamento quanto alle autorità di controllo che devono monitorarli. Pertanto, in un mondo dove la natura delle informazioni cambia frequentemente, non è più possibile limitare la valutazione del rischio – generalmente inteso e non limitato esclusivamente alla c.d. "valutazione d'impatto sulla protezione dei dati" prevista dall'art. 35 del GDPR – alle sole ipotesi di dati personali, ma appare opportuno, se non necessario, estenderla a tutti i dati che il medesimo soggetto ha a disposizione, includendo anche quelli non personali[137]. Purtroppo, è proprio l'assenza di una visione onnicomprensiva capace di tenere conto della mutevolezza della realtà digitale a minare l'efficacia delle disposizioni del RDNP, le quali non riescono a soddisfare l'esigenza di coordinamento con il Regolamento generale sui dati personali.

Questo particolare deficit potrebbe ripercuotersi negativamente sulla effettività della libera circolazione di tutti i tipi di informazione sia all'interno che all'esterno dell'Unione. In primo luogo, risultano evidenti le problematicità che dovrebbe affrontare il titolare del trattamento desideroso di usufruire delle possibilità offerte dal RDNP giacché, malgrado l'assenza di un obbligo diretto di separazione del dataset, si vedrebbe costretto a scindere il suo insieme in due parti: una costituita da dati personali che, ipoteticamente, potrebbe essere sottoposta ad una misura restrittiva della circolazione – motivata da ragioni diverse dalla protezione dei dati – mentre l'altra parte, contenente dati non personali, potrebbe essere trasferita liberamente[138]. Di conseguenza, graverebbe sul titolare del trattamento un onere aggiuntivo ed implicito che, prescrivendo di fatto un'operazione costosa e di difficile riuscita[139], rischia di incentivare quell'atteggiamento di chiusura che il Regolamento mira ad eliminare[140].

In secondo luogo, l'interpretazione fornita dalla Commissione che, nel tentativo di dare precedenza alla tutela dei dati personali, propende per un'applicazione aprioristica del regime più restrittivo previsto dal GDPR nei confronti degli insiemi dei dati misti, potrebbe condurre ad un'ulteriore barriera indiretta alla libera circolazione dei dati non personali, trasformandosi in buona sostanza proprio in una misura di *data localization*[141].

In ultima analisi, la delicatezza del problema degli insiemi di dati misti e le difficoltà nel gestire le conseguenze di una regolamentazione così scarna si possono osservare anche con riferimento alla questione della portabilità, dove la predisposizione di una tutela a due livelli suscita alcune perplessità. Innanzitutto, se i codici di condotta non riconosceranno un vero e proprio diritto di portabilità, l'utente professionale intenzionato a spostare presso un nuovo *provider* l'intero insieme, senza procedere ad una complicata separazione, rischierebbe di dover affrontare un lungo contenzioso con il precedente fornitore del servizio i cui tempi di risoluzione sono del tutto inconciliabili con la velocità a cui procede la società digitale[142]. Oltretutto, anche nell'ipotesi in cui venisse riconosciuto dai codici di condotta e da clausole contrattuali, la prevalenza di una prerogativa di questo genere non può essere data per certa nell'eventualità in cui dovesse entrare in conflitto con altri diritti espressamente stabiliti dalla lettera della legge[143], in particolare con quelli più maturi e radicati nel mondo digitale – ad esempio, la proprietà intellettuale, i segreti commerciali o i diritti connessi alla tutela giuridica delle banche dati[144].

6. La necessità di una visione onnicomprensiva per la realtà digitale moderna

L'economia globale ed interconnessa che caratterizza la nostra epoca si basa su un incessante scambio di informazioni che partono ed arrivano in tutte le parti del mondo in tempi praticamente nulli. In risposta al rapido aumento del valore economico e dell'importanza strategica dei dati, sia personali che non, si è assistito ad una crescita del sentimento di sfiducia fra gli Stati, sfociato poi nell'adozione di normative aventi ad oggetto obblighi di localizzazione. Di fronte ad un cambiamento di simile portata, l'ordinamento giuridico europeo ha deciso fronteggiare la sfida posta dal fenomeno della *data localization* non attraverso un'iniziativa singolare ed unica, ma seguendo un percorso a tappe, in linea con la gerarchia di valori della tradizione giuridica continentale. In prima battuta, il legislatore ha deciso di predisporre una tutela elevata all'interno dell'Unione europea per quanto riguarda il trattamento dei dati personali. Partendo da tale presupposto, ha poi elaborato un insieme di regole che, per un verso, incentivasse la circolazione di tali dati sul suolo continentale e, per l'altro, permettesse alla tutela di viaggiare con il dato personale anche quando questo viene trasferito verso Paesi terzi.

La disciplina riguardante l'altro versante del *data law*, quello del dato non personale, ha visto la luce in un secondo momento, quando il peso della mancanza di una normativa completa a sostegno dell'economia europea dei dati non era di fatto più sostenibile. Sfortunatamente, il Regolamento sulla libera circolazione dei dati non personali non sembra avere soddisfatto le aspettative, in quanto non riesce a fornire un quadro normativo sufficientemente aderente alle dinamiche della realtà digitale.

Allargando lo sguardo all'impianto generale in materia di dati, la critica principale che può muoversi nei confronti del legislatore europeo concerne la carenza di una risistemazione in chiave organica di tutta la disciplina. Attualmente, l'ordinamento continentale consta di una vasta gamma di normative settoriali e, in alcuni casi, non coordinate, la cui stratificazione nel corso dell'ultimo decennio rischia di confondere l'interprete e di tradursi in uno strumento non adatto a servire lo sviluppo della società digitale[145]. Le lacune patite dal Regolamento sui dati non personali non rappresentano altro che il precipitato ultimo di questa disordinata ipertrofia normativa: nonostante l'apparente complementarietà, le sue disposizioni sono state concepite come facenti parte di un *corpus* separato rispetto al Regolamento generale sulla protezione dei dati personali, in evidente contrasto con quella visione di insieme che è ormai imprescindibile se si vuole regolamentare il mondo virtuale con la speranza di ottenere risultati concreti. Viceversa, il RDNP rischia di diventare un regolamento senza oggetto in quanto l'assenza di una impostazione sistemica che tenga conto della preponderanza degli insiemi di dati misti e, soprattutto, delle caratteristiche dei soggetti che trattano questi insiemi, non permette di inquadrare il problema nella prospettiva idonea ad attribuire al dato non personale l'importanza che merita. In aggiunta, oltre alla prevalenza schiacciante del GDPR patita dal Regolamento sui dati non personali, non sono da sottovalutare le ulteriori problematiche di coordinamento di questi due regolamenti con le altre discipline settoriali che, spesso, prescindono dalla distinzione personale-non personale[146].

La risoluzione degli interrogativi che inevitabilmente emergono da questa confusione normativa è posta totalmente a carico del soggetto che gestisce i dati, il quale, disorientato in un labirinto di regole, si rifugerà nei lidi più sicuri, ma anche più costosi, dell'internalizzazione del trattamento dei dati. Tuttavia, è bene ricordare, simili pratiche non sono economicamente sostenibili da parte delle piccole e medie imprese che, ancora una volta, saranno costrette a pagare le conseguenze di disposizioni normative non coordinate adeguatamente fra loro.

Note

[1] OCSE, *Data-driven innovation. Big data for growth and well-being*, OCSE Publishing, Parigi, 2015.

[2] A. McAfee, E. Brynjolfsson, *Big data: the management revolution*, in "Harvard Business Review", 2012, n. 10.

[3] H.A. Ünver, G. Kim, *Cross-border data transfers and data localization*, EDAM Cyber Policy Paper Series, 2016, n. 3, p. 2-6.

[4] M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, ECIPE occasional paper, 2014, n. 3, p. 3-10.

[5] M.F. Ferracane, *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper, 2017, n. 1, p. 6.

[6] M.L. Montagnani, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in "Mercato concorrenza regole", 2019, n. 2, pp. 311-313.

[7] M.F. Ferracane, *op. cit.*, p. 2-3.

[8] Come, ad esempio, accade in Russia. Per un approfondimento, si veda A. Savelyev, *Russia's new personal data localization regulations: a step forward or a self-imposed sanction?*, in "Computer Law & Security Review", 2016.

[9] M.F. Ferracane, *op. cit.*, p. 2-3.

[10] *Ibidem.*

[11] *Ibidem.* Naturalmente, la realtà dei fatti non rispecchia così nettamente la classificazione appena svolta, giacché le differenze possono essere molto più labili di quanto si pensi, ed

anche una misura condizionale può facilmente tramutarsi in rigida se l'iter necessario ad addivenire al trasferimento è troppo oneroso per la dimensione in cui opera il trasferente.

[12] *Ivi*, p. 8-9.

[13] M. Bauer, H. Lee-Makiyama, E. van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, cit., p. 5-10.

[14] P.S. Ryan, R. Falvey, S. Merchant, *When the cloud goes local: the global problem with data localization*, in "Computer", Vol. 46, 2013, n. 12, p. 54-59; A. Chander, U.P. Le, *Breaking the web: data localization vs. the global internet*, Working Paper, 2014, n. 1, p. 10-16; European Commission, *Cross-border data flow in the digital single market: study on data location restrictions* (SMART n. 2015/0054), Publication Office of the EU, 2017.

[15] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa* - COM(2015) 192 final, pp. 15-21.

[16] La relatrice del Parlamento europeo Anna Maria Corazza Bildt, a seguito dell'approvazione del Regolamento (UE) 2018/1807, ha affermato che è stata introdotta una "quinta libertà di circolazione" che riguarda tutti i dati.

[17] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti* - COM(2017) 228 final, 2017, pp. 23-26.

[18] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, ECIPE policy brief, 2016, n. 3, pp. 12-13. In particolare: «A ban on data localisation is a powerful political message that the Single Market is open for business. This argument is particularly pertinent as the EU seeks to convince the market and turn the tide on the digital investments, and both inward and domestic investments into Europe's digital economy are withheld or diverted to other regions».

[19] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente* - COM(2011) 882 final, pp. 7-8. In particolare: «Nonostante l'armonizzazione minima introdotta dalla direttiva del 2003 sul riutilizzo delle informazioni del settore pubblico, permangono differenze significative nelle norme e pratiche nazionali, con conseguente frammentazione del mercato interno dell'informazione e presenza di ostacoli alla creazione di servizi di informazione transfrontalieri».

[20] A tal proposito, è opportuno ricordare che, nonostante la tematica dei dati personali stesse prendendo piede, la prima proposta ufficiale emanata dalla Commissione con riguardo alla riforma della disciplina della protezione dei dati personali è datata gennaio 2012.

[21] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente*, cit., pp. 5-6.

[22] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Verso una florida economia basata sui dati* - COM(2014) 442 final, pp. 12-13.

[23] Per un'analisi dettagliata del percorso che ha condotto all'istituzionalizzazione del diritto alla protezione dei dati personali, si vedano: G. Gonzalez Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014; G.F. Aiello, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in "Osservatorio del diritto civile e commerciale", 2015, n. 2.

[24] L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in "diritticomparati.it", 2014, pp. 8-13.

[25] Per un approfondimento, si vedano: H. De Hert, V. Papakonstantinou, *The data protection regime in China. In-depth analysis for the LIBE Committee*, Publication Office of the EU, 2015, p. 13-27; Z. Yuexin, *Cyber protection of personal information in a multi-layered system*, in "Tsinghua China Law Review", 2019, n. 1.

[26] 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.

[27] C. Colpaert, M.-C. Janssens, *Work in progress: the proposal of the free flow of non-personal data regulation*, KU Leuven - CITIP Blog, 2018.

[28] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea* - COM(2017) 9 final, pp. 9-14.

[29] *Ivi*, pp. 2-5.

[30] *Ibidem*.

[31] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Comunicazione "Verso uno spazio comune europeo dei dati"* - COM(2018) 232 final, p. 1.

[32] M.L. Montagnani, *op. cit.*, pp. 298-302.

[33] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[34] Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione.

[35] Commissione europea, *Documento di lavoro dei servizi della Commissione. Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso uno spazio comune europeo dei dati"* - SWD(2018) 125 final.

[36] M.L. Montagnani, *op. cit.*, pp. 298-302.

[37] S. Kirschen, *Il trasferimento all'estero dei dati*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018", Giuffrè, 2019, pp. 265-268.

[38] Regolamento (UE) 2016/679, considerando n. 13. In particolare: «Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione

non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[39]Regolamento (UE) 2016/679, art. 1, par. 3: «La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[40]M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit., p. 3-8.

[41]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[42]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* - COM (2019) 250 final, p. 15, dove è riportato un esempio eloquente al riguardo: «Una normativa nazionale prevede che la contabilità del personale sia situata in uno specifico Stato membro per ragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale non rientrerebbe nell'ambito di applicazione dell'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati, in quanto i motivi non riguardano la protezione dei dati personali. Questo obbligo dovrebbe invece essere valutato sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea».

[43]Gli esempi generalmente riportati fanno riferimento, ma non sono limitati, a: Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno; Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[44]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 14-15.

[45]Tra le sentenze più significative, si ricordano: Corte di Giustizia UE, 13 maggio 2014, causa C-131/12; Corte di Giustizia UE, 6 ottobre 2015, causa C-362/14; Corte di Giustizia UE, 28 luglio 2016, causa C-191/15. Per una panoramica generale sull'evoluzione della giurisprudenza della Corte di giustizia, si veda: S. Calzolaio, voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017, pp. 620-624.

[46]Institute of International Finance, *Data flows across borders. Overcoming data localization restrictions*, 2019.

[47]Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato* – COM(2017) 7 final, pp. 4-6. In particolare: «L'obiettivo principale di tali norme è garantire che, quando i dati personali dei cittadini europei vengono trasferiti all'estero, la tutela viaggi con loro».

[48]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*, cit., pp. 23-26.

[49]V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 4-5, pp. 683-695; L. Valle, L. Greco, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in "Il diritto dell'informazione e dell'informatica", 2017, n. 2, pp. 198-201; S. Kirschen, *op. cit.*, pp. 265-268.

[50]Regolamento (UE) 2016/679, art. 44.

[51]S. Kirschen, *op. cit.*, pp. 261-265.

[52]M.F. Ferracane, *op. cit.*, p. 5.

[53]Regolamento (UE) 2016/679, art. 45, par. 1: «Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche».

[54]S. Kirschen, *op. cit.*, pp. 261-272; L. Valle, L. Greco, *op. cit.*, pp. 188-191.

[55]Infatti, l'articolo 49, paragrafo 5 del GDPR recita: «In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione». S. Kirschen, *op. cit.*, pp. 283-291.

[56]*Contra*, L. Valle, L. Greco, *op. cit.*, pp. 218-219. In particolare: «[...] per quanto concerne l'altro profilo della regolazione transfrontaliera dei dati personali relativo al trasferimento verso Paesi terzi esso è legato a dei canoni, come quello del controllo dell'adeguatezza della disciplina del Paese terzo e della decisione sull'adeguatezza di clausole standard da parte della Commissione europea, che poco si adattano ad un flusso di dati quale quello che si reputa conveniente allo sviluppo delle attività economiche nel mondo contemporaneo».

[57] S. Kirschen, *op. cit.*, pp. 283-291.

[58]L'elenco delle deroghe di cui all'articolo 49 del GDPR ricomprende: il consenso esplicito dell'interessato, l'esecuzione o la conclusione di un contratto in cui l'interessato è parte o beneficiario, importanti motivi di interesse pubblico, difesa o esercizio di un diritto in sede giudiziale, interessi vitali, quando le informazioni sono contenute in un registro aperto alla consultazione pubblica e, infine, interessi legittimi cogenti del titolare del trattamento.

[59]European Data Protection Board (EDPB), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 2018. Invero, il Comitato, forzando il significato letterale del testo, afferma che i concetti di "occasionalità" e "non ripetitività" indicati con riferimento alla sola eccezione relativa agli interessi legittimi cogenti del titolare del trattamento, devono essere applicati a tutte le ipotesi previste nell'articolo, anche se non indicato esplicitamente.

[60]S. Kirschen, *op. cit.*, pp. 274-283.

[61]L'articolo 4, punto 20, del GDPR definisce le norme vincolanti d'impresa come «le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune». Pertanto, tali norme sono

costituite da quell'insieme di regole, politiche e strumenti applicabili (solamente) all'interno delle società del gruppo al fine di assicurare il rispetto dei principi, dei diritti e degli obblighi riguardanti la protezione dei dati personali nell'Unione europea. Per un approfondimento si veda, G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al safe harbor agreement?*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai «Safe Harbour Principles» al «Privacy Shield»", Tre Press, 2016.

[62]Tuttavia, il loro impiego non era sconosciuto prima dell'avvento del GDPR, tanto che il Gruppo di lavoro Articolo 29 si era già espresso a tale riguardo nel 2003: Article 29 Data Protection Working Party (WP29), *Working document: transfers of personal data to third countries: applying article 26 (2) of the EU data protection directive to binding corporate rules for international data transfers* (WP74).

[63]S. Kirschen, *op. cit.*, pp. 274-283.

[64]*Ibidem*.

[65]Per una visione critica (e metaforica) del meccanismo europeo, si veda: A. Mantelero, *From "safe harbour" to "privacy shield". The "medieval" sovereignty on personal data*, in "Contratto e Impresa/Europa", 2016, n. 1.

[66]C. Focarelli, *Privacy. Proteggere i dati personali oggi*, Il Mulino, 2015, pp. 123-175.

[67]Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[68]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[69]A tal proposito, è doveroso osservare che, nonostante il considerando 9 del Regolamento sembri accennare ad una definizione concreta della nozione di dato non personale, il suo carattere meramente esemplificativo non permette di trarre conclusioni inequivocabili al riguardo.

[70]Gli esempi riportati dalla Commissione sono quelli dei dati sulle condizioni meteorologiche prodotti da sensori o i dati sulle esigenze di manutenzione delle macchine industriali.

[71]Lo stesso documento sottolinea sin da subito il carattere puramente informativo della guida della Commissione: «Il presente documento è fornito dalla Commissione europea esclusivamente a titolo informativo. Esso non contiene alcuna interpretazione autorevole del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, né costituisce una decisione o un'opinione della Commissione europea. Tale documento non pregiudica eventuali decisioni o opinioni della Commissione europea, né le competenze della Corte di giustizia dell'Unione europea per l'interpretazione del regolamento conformemente ai trattati dell'UE».

[72]S. Stalla-Bourdillon, *A. Knight, Anonymous data v. personal data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in "Wisconsin International Law Journal", 2017, n. 2; G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017.

[73]Il GDPR, come indicato al considerando 27, esclude i dati dei deceduti dal suo ambito di applicazione ma, al contempo, permette ai singoli Stati membri di adottare una scelta differente, disciplinando questo tipo di informazioni alla stregua di quelle a carattere personale (come avviene in Italia, ex art. 2-terdecies, d.lgs. 30 giugno 2003, n. 196). Di fatto, la discrezionalità riconosciuta ai singoli legislatori nazionali, legittimando una classificazione normativa differente dello stesso tipo di informazione, potrebbe portare alla creazione di ambiti normativi non totalmente coincidenti all'interno dell'unico ordinamento giuridico europeo.

[74]S. Calzolaio, voce *Protezione dei dati personali*, cit., pp. 605-608; S. Forge, *Optimal scope for free-flow of non-personal data in Europe*, IPOL, 2016, p. 1-6; I. Grae, R. Gellert, M. Husovec, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation*, in "European Law Review", 2019, n. 5, p. 605-621.

[75]M.L. Montagnani, *op. cit.*, pp. 304-310.

[76]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 15-16. In particolare: «Il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea non riguarda gli obblighi di localizzazione di dati imposti dagli Stati membri sull'archiviazione dei dati non personali in un paese terzo, che possono essere presenti negli ordinamenti giuridici nazionali».

[77]*Parere del Comitato economico e sociale europeo (CESE) sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, p. 6. In particolare: «Inoltre, la proposta della Commissione non tiene debito conto della natura globale e transeuropea dell'economia digitale e si preoccupa solo di regolamentare il mercato interno, dimenticando che quest'ultimo si sviluppa in un mercato globale, senza alcuna garanzia che gli altri paesi e continenti seguano le stesse regole che essa stessa intende attualmente applicare e senza il potere di imporle nei negoziati internazionali».

[78]Regolamento (UE) 2018/1807, considerando n. 4.

[79]La figura dell'"utente professionale" è definita dal punto 8, dell'articolo 3 del Regolamento come: «una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione».

[80]Regolamento (UE) 2018/1807, considerando n. 6.

[81]European Commission, *Staff working document impact assessment, Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"* - SWD (2017) 304 final, part 1/2.

[82]L'articolo 4, rubricato *Libera circolazione dei dati all'interno dell'Unione*, al paragrafo 1 stabilisce: «Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Il primo comma del presente paragrafo fa salvo il paragrafo 3 e gli obblighi di localizzazione dei dati stabiliti sulla base del diritto vigente dell'Unione».

[83]Regolamento (UE) 2018/1807, art. 3, punto 5.

[84]European Commission, *Commission staff working document impact assessment. Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"*, cit.

[85]European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Questo studio molto approfondito identifica gli obblighi di localizzazione che si possono trovare in alcuni Stati membri dell'Unione europea, p. 18.

[86]A titolo esemplificativo, possono essere citate due fra le più recenti barriere dirette introdotte dal legislatore italiano. La prima è contenuta nel d.l. 21 settembre 2019, n. 105,

recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica» convertito in l. 18 novembre 2019, n. 133, il quale, tramite la creazione di un perimetro di sicurezza nazionale cibernetica, potrebbe limitare la circolazione di informazioni inerenti all'esercizio di "una funzione essenziale dello Stato" oppure alla "prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale». La seconda barriera, invece, può rinvenirsi nell'art. 6 del d.l. 30 aprile 2020, n. 28 convertito in l. 25 giugno 2020, n. 70, recante «Misure urgenti per l'introduzione del sistema di allerta Covid-19», che istituisce una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti che usufruiscono della app "Immuni". Per un approfondimento, si rinvia a S. Calzolaio, *Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020*, in E. Calzolaio, M. Meccarelli, S. Pollastrelli (a cura di), "Il diritto nella pandemia. Temi, problemi, domande", Macerata EUM, 2020.

[87] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Lo studio tiene comunque a precisare che le barriere indirette sono state considerate tali alla luce delle valutazioni fatte da esperti del settore.

[88] *Ivi*, p. 6.

[89] *Ibidem*.

[90] *Ivi*, p. 103. Nello specifico, lo studio recita: «More numerous were the indirect data location requirements, which included the accessibility of data to specific supervisors or regulators, the definition of generic technical requirements, prior authorisation schemes for infrastructure or service providers, the mandatory use of a specific infrastructure, data segregation requirements, subcontracting restrictions, and data destruction requirements».

[91] Merita evidenziare che, mentre il Regolamento generale sulla protezione dei dati personali ha come base giuridica l'articolo 16 TFUE, il Regolamento relativo alla libera circolazione dei dati non personali è stato adottato sulla base dell'articolo 114 TFUE, il quale attribuisce al Parlamento ed al Consiglio la competenza ad adottare «le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno».

[92] Regolamento (UE) 2018/1807, considerando n. 4. In particolare: «Il presente regolamento non limita in alcun modo la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati. Il presente regolamento è inteso unicamente a salvaguardare tale libertà garantendo che il luogo stabilito possa trovarsi ovunque nell'Unione».

[93] Regolamento (UE) 2018/1807, considerando n. 14. In particolare: «Mentre le autorità pubbliche e gli organismi di diritto pubblico sono incoraggiate a considerare i vantaggi economici e di altro tipo dell'esternalizzazione a fornitori esterni di servizi, essi potrebbero avere ragioni legittime per scegliere l'autofornitura di servizi o l'internalizzazione. Di conseguenza, il presente regolamento non obbliga in alcun modo gli Stati membri a subappaltare o esternalizzare la fornitura di servizi che essi intendono fornire direttamente o organizzare con mezzi diversi dagli appalti pubblici».

[94] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. p. 17. In particolare: «These barriers can of course take many forms. In some cases, there is a clear and objective compliance requirement behind them, such as a legal obligation to store data locally in order to maintain national control over essential systems and services. In other cases, a barrier can result from business requirements (e.g. customer demand to store data locally), policy preferences (e.g. a desire to keep data within one's own jurisdiction), operational needs (e.g. a requirement to be able to destroy data), or even personal preferences (e.g. favouring local companies) and personal concerns (e.g. concern that foreign entities may seize data stored abroad)».

[95] IDC, Open Evidence, *European data market study*, Final Report (SMART 2013/0063), 2017.

[96] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit.

[97] Regolamento (UE) 2018/1807, considerando n. 10. In particolare: «Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati».

[98] La proposta congiunta lanciata dai Ministeri dell'economia tedesco e francese di creare una infrastruttura digitale di matrice europea, denominata GAIA-X, rispondente ai valori continentali di sicurezza e tutela dei dati è evidentemente diretta a ridurre la dipendenza nei confronti dei fornitori di servizi non europei e ad incentivare la concorrenza. In tal senso, *GAIA-X: A pitch towards Europe. Status report on user ecosystems and requirements*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

[99] La predisposizione di una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti della app "Immuni" nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19 rappresenta una chiara presa di posizione da parte del legislatore italiano, il quale ha preferito una soluzione con titolarità pubblica e con infrastrutture localizzate sul territorio nazionale. Per un approfondimento, si rinvia a: C. Colapietro, A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in "Dirittifondamentali.it", 2020, n. 2.

[100] A tal proposito, eloquente è il caso dei *Community Mobility Reports* messi a disposizione da Google per fornire una panoramica della variazione degli spostamenti della popolazione durante la pandemia causata dal Covid-19, i quali dimostrano quanto sia pervasiva e vasta la raccolta e l'analisi dei dati realizzata dai servizi OTT.

[101] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21. La medesima procedura è prevista al paragrafo 2 nell'eventualità in cui gli Stati intendano introdurre un nuovo obbligo dello stesso tenore.

[102] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21.

[103] Per le sentenze della Corte di giustizia dell'Unione europea più rilevanti a tale riguardo, si rinvia alla European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 13.

[104] M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in "federalismi.it", 2016, n. 23.

[105] Regolamento (UE) 2018/1807, considerando n. 19. A tale riguardo, il rischio di difformità nelle normative degli Stati membri che potrebbe derivare da questa facoltà di deroga si aggiunge a quello dovuto alla scelta, da parte del legislatore, di ricorrere allo strumento della direttiva per disciplinare il trattamento dei dati personali effettuato da autorità pubbliche in ambito penale. In particolare, ci si riferisce alla Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali

ed alla Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[106] L. Tarantino, *Promozione della concorrenza e disciplina dei servizi pubblici*, 2016, pp. 8-11; A. Di Giovanni, *I servizi di interesse generale tra poteri di autorganizzazione e concessione di servizi*, Giappichelli, 2018, pp. 1-17.

[107] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit.

[108] *Parere del CESE sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"*, adottato il 25 settembre 2019.

[109] M. Nino, *Il caso "Datagate". I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in "Diritti umani e diritto internazionale", 2013, n. 3, pp. 735-737.

[110] C. Focarelli, *op. cit.*, pp. 10-16.

[111] C. Kuner, F.H. Cate, C. Millard, D.J.B. Svantesson, *Systematic government access to private-sector data redux*, in "Articles by Maurer Faculty, Indiana University", 2014, n. 4. Due eccezioni degne di nota sono quelle di Microsoft ed Apple che si sono opposte alle richieste di accesso da parte delle autorità statunitensi, si veda M. Rubechi, *op. cit.*, p. 23.

[112] Ci si riferisce all'articolo 9 del Regolamento (UE) 2016/679, rubricato *Trattamento di categorie particolari di dati personali*.

[113] Prima dell'abrogazione, la Legge n. 675 del 31 dicembre 1996 relativa alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, all'articolo 22, riportava la rubrica "Dati sensibili". Anche il Decreto legislativo 30 giugno 2003, n. 196, riportava la medesima dicitura prima della modifica ad opera del decreto legislativo 101 del 2018 relativo alle disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

[114] Un concetto simile è presente nell'ordinamento giuridico della Repubblica popolare cinese dove viene in rilievo la nozione di *important data*, la quale, benché possa comprendere sia dati personali che non, appronta una disciplina più rigida proprio in virtù della particolare importanza di queste informazioni in riferimento alla sicurezza, all'economia o alla stabilità sociale del Paese. A questo proposito, si veda Z. Yuexin, *op. cit.*, p. 159-169.

[115] Regolamento (UE) 2018/1807, considerando n. 29.

[116] European Commission, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy* - SWD(2017) 2 final, p. 46-49.

[117] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[118] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[119] Regolamento (UE) 2018/1807, considerando n. 30.

[120] *Parere del CESE sulla "Comunicazione della Commissione*, cit. Per un'analisi dettagliata del diritto alla portabilità che ne include gli eventuali effetti negativi, anche se con riferimento ai dati personali, si veda: P. Swire, Y. Lagos, *Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique*, in "Maryland Law Review", 2013, n. 2, p. 335-380.

[121] Nelle versioni italiane viene impiegato il medesimo termine, "portabilità", in entrambi i regolamenti.

[122] L. Miglietti, *op. cit.*, pp. 8-13.

[123] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[124] *Ibidem*.

[125] Il rapporto giuridico sussistente tra utente professionale e fornitore del servizio non sempre può essere declinato all'interno della dinamica titolare-responsabile del trattamento come delineata dal GDPR, poiché l'assunzione di tali ruoli ha luogo solamente se sono coinvolti (anche) dati a carattere personale.

[126] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[127] J. Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016, p. 55-66; T. Fia, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in "Nuovo Notiziario Giuridico", 2019, n. 1, pp. 125-126; *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[128] M.L. Montagnani, *op. cit.*, pp. 304-310; *Parere del CESE sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, cit., pp. 5-6. In particolare: «In questo senso, il CESE ritiene che il regolamento all'esame dovrebbe almeno fornire un insieme di norme di base relative ai rapporti contrattuali tra i fornitori di servizi e gli utenti e prevedere una lista nera di clausole vietate a causa della limitazione del diritto di portabilità, secondo i parametri indicati in particolare nel suo parere sull'autoregolamentazione e sulla co-regolamentazione. Tuttavia, è inconcepibile che la Commissione non abbia neppure proposto di definire «orientamenti» per l'elaborazione dei codici di condotta precedentemente citati, come ha già fatto in altri settori, sostenuta in questo approccio dal CESE».

[129] Particolarmente azzeccata è l'osservazione secondo la quale è «anche dall'efficacia del Regolamento [sulla libera circolazione dei dati non personali] che si misura quella dell'intero quadro regolatorio sulla libera circolazione dei dati», in M.L. Montagnani, *op. cit.*, p. 304.

[130] Il termine "insiemi di dati misti", che compare in diversi documenti antecedenti all'approvazione del Regolamento, è stato poi ripreso dalla Commissione europea nelle Linee guida di maggio 2019.

[131] Riprendendo le parole della commissione, l'ipotesi dell'insieme indissolubilmente legato ricorre quando questo «contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile», European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 10. Regolamento (UE) 2018/1807, art. 8.

[132] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[133] Regolamento (UE) 2018/1807, art. 8.

[134] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[135] G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in S. Sica, V. D'antonio, G.M.

Riccio, "La Nuova Disciplina Europea Sulla Privacy", Wolters Kluwer, 2016, pp. 55-78; A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in "Le Nuove Leggi Civili Commentate", 2017, 1, pp. 144-164.

[136] M. Finck, F. Pallas, *They who must not be identied – distinguishing personal from non-personal data under the GDPR*, in "International Data Privacy Law", 2020, n. 1, p. 11-36.

[137] A tal proposito, sia consentito rinviare a S. Torregiani, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18, pp. 317-341.

[138] C. Flynn, *Shortcomings of the EU proposal for free flow of data*, in "InterMEDIA", 2018, n. 4, p. 30-35.

[139] Le difficoltà insite nell'identificazione del tipo di dato che si sta trattando non permettono sempre di raggiungere un risultato esatto in senso assoluto. In proposito, S. Forge, *op. cit.*, p. 1-6.

[140] M.L. Montagnani, *op. cit.*, pp. 304-310.

[141] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[142] *Ibidem.*

[143] Nonostante durante l'ultimo decennio si siano ritagliati uno spazio importante nell'ordinamento europeo, non è ancora chiaro quale natura giuridica debba essere riconosciuta ai codici di condotta. Le linee guida fornite dal Comitato europeo per la protezione dei dati definiscono i codici di condotta previsti dal GDPR, nello specifico all'articolo 40, come "strumenti di responsabilizzazione volontari" che possono rivelarsi utili "in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore" (così European Data Protection Board, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679, 2019).

[144] J. Drexl, *op. cit.*

[145] M.L. Montagnani, *op. cit.*, pp. 311-313.

[146] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

* * *

The European legal framework for the free flow of data. The peril of a regulatory burden

Abstract: The increase in the free flow of data due to the digitalization has been followed by an even relevant growth of data localization restrictions required by EU member States legislative or administrative measures. The European legislator, willing to build a digital single market where all data can flow freely across EU, decided to face the data localization phenomenon through many different and sector-specific interventions, mainly based on the – still blurred – distinction between personal and non-personal data. Thanks to the analysis of the main sources of the European legal framework, this paper will assess if this patchwork, chosen over an overarching approach, is the most adequate for the common European data space.

Keywords: Free flow of data – Data localization – Personal data – Non-Personal Data

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0028

Cross-border Data Transfer Regulation in China

Yuan Li

With the growing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being disintegrated and reshaped. It is of particular importance for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules. China keeps leveraging the data sovereignty to fasten the law-makings to support the development of critical technology in digital domains and infrastructure construction. This paper aims to systematise Chinese regulations for cross-border data exchange following the chronological order. The enacted and draft provisions as well as binding and non-binding regulatory rules are studied, and various positive dynamic developments in the framing of China's cross-border data regulation are shown. Despite certain limitations, the Cybersecurity Law, together with Civil Code and Personal Information Protection Law, demonstrates great willingness towards a stronger data protection regime and more flexible regulatory mechanism.

China – Cross-border data flow – Cybersecurity

Sommario: *1. Introduction – 1.1. Global Data Transfer – 1.2. Problem Statement – 2. The Evolution of China's Personal Data Protection Laws – 2.1. Cybersecurity Law – 2.2. Enforcement and Authorities – 3. Data Export Regulations – 3.1. Critical Information Infrastructure Data Export – 3.2. Personal Information Export – 4. Conclusion*

1. Introduction

The regulation of cross-border data transfers represents one of the greatest challenges that data protection experts and legislators are facing around the world[1]. The global data protection law regime is fragmented by the divergence among various data protection standards. The potential negative effects shall not be undermined. From the perspective of countries, the adoption of the "adequate level of protection" approach *de facto* restricts the less developed regions, especially those that have not enacted data protection laws, from entering the global data flows. It further leads to the elimination of such countries from participating in global digital trade and exacerbates the polarization of the world economy. From the perspectives of entities, particularly those in the Information Communication Technology (ICT) sector, the legal requirements set out in different jurisdictions are likely to impose additional administrative and technical burdens when conducting business internationally. The overlapping jurisdictions over various countries, cumbersome transfer assessment rules, and excessive discretionary powers of supervisory authorities have led to increased compliance costs while reducing the transaction efficiency of multinational businesses. From the perspective of data subjects, individuals' rights and

Y. Li is Early Stage Researcher in the framework of the HEART project (*HEalth related Activity Recognition system based on IoT – an interdisciplinary training program for young researchers*), at the University of Macerata (Italy). The HEART project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 766139. This article reflects only the author's view and the REA – Research Executive Agency is not responsible for any use that may be made of the information it contains. This essay is part of the monographic section *Ubi data, ibi imperium: public law facing data localization* edited by Simone Calzolaio.

responsibilities vary from nationality, residence, or information collection region. It is, however, contrary to the original purpose of protecting personal data while promoting data sharing.

1.1. Global Data Transfer

The benefits that can be derived from cross-border data flows are growing, while the ability of countries to reap such benefits may vary[2]. Although it is widely recognized that countries should have a common interest in facilitating cross-border data flows and reconciling different policy objectives in this field, the implementation of the free flow of cross-border data remains vague. Due to the differences lay in digital economic development, legal systems, and data sovereignty objectives, it is difficult for countries to impose effective regulations on cross-border data transfer through one's own. In contemporary legislations, a trend of preference for establishing one data flow model inside a region within a given group of countries is emerging.

Multilateral international agreement

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted by the Council of Europe in 1981 is the first and up-to-date only binding multilateral international agreement to set standards for the transborder data flows. The early version of Convention 108 provides general principles that require signatory countries not to restrict or impose any special authorisations to prevent the flow of personal data among the member states and aims to achieve greater unity between its members[3]. The Convention 108 was further developed in the Additional Protocol in 2001 to introduce the concept of an "adequate level of protection" for the intended data recipient countries that are not the signatories to Convention 108[4]. Such exporting party is also subject to exceptions where the transfer is in the need of individual's legitimate interests and public interest, or is based on authority-approved contractual clauses.

The Convention 108 is the result of the implementation of the European Convention on Human Rights with regard to privacy protection. It attempts to build consistent data protection principles to safeguard individual's rights while keeping active exchanges of such personal information across the borders. Be great as it may, the significance of Convention 108 is limited[5]. Although international agreement as an instrument for dealing with modern societal and legal topics is advantageous in terms applicable scope of the rules, enforcement and guidance, its complex and lengthy establishment procedures have slowed down the reaction time to the emerging issues in international community, especially in areas where international consensus has not yet been reached.

Bilateral international agreement

In view of the latency of the international community's cooperation in the field of cross-border personal data transfer, multiple emerging countries in digital economy have actively launched bilateral negotiations based on their own development needs. By reaching the bilateral agreement, it is provided with a legal basis for the personal data exchanges between the signatory countries. The EU-U.S. Privacy Shield Framework is an example. In 2014, being the direct response to the Snowden revelations, *Schrems I* case led to the revocation of the Safe Harbor as a valid mechanism for transfers between the EU and the U.S. by the Court of Justice of European Union (CJEU)[6]. The EU and the U.S. successfully reached the Privacy Shield Framework as the alternative, putting forward more stringent and descriptive data transfer requirements for data controllers[7]. After receiving wide critics, the EU Commission's adequacy determination for the Privacy Shield was rendered[8]. American companies may be permitted to acquire personal data from a total of 28 European countries after being registered under the Privacy Shield program and demonstrated that they fulfil the "adequacy protection" requirement by self-certify procedures. Privacy Shield Framework additionally includes verification, assessment and supervision mechanisms, as well as special rules related to arbitration procedures[9]. The bilateral agreement allows two countries to make more detailed arrangements for cross-border data transfer issues. It is advantageous in terms of negotiation efficiency and enforcement, as well as the flexibility of contents. Yet, its scope of application is limited to the jurisdictions of the two countries. For the establishment of a regional framework of personal data cross-border transfer, bilateral agreement has very limited effect on bridging different legal standards.

Soft laws

Soft laws often play important roles in encouraging reluctant states to consider and eventually agree upon policies and strategies in areas where serious differences exist. Many international organisations have issued soft laws to regulate cross-border transfer of personal data, which has given certain guidance to the national legislation and implementation. The OECD Privacy Guidelines released in 1980 serve as the first internationally agreed upon set of personal

information protection principles and focus on balancing between the needs for digital economy and the protection of individual's rights. It addressed the needs for greater efforts to tackle the global dimension of privacy through improved interoperability and provided the member states a basic framework of free flow of personal data for further negotiations. The APEC framework, published by the Asia-Pacific Economic Cooperation in 2004, is a framework to protect privacy while enable regional personal information transfers to promote consumer trust and business confidence, to lighten compliance burdens and booster digital economy. The data controllers' obligations are particularly emphasised as data subject's consent is mandatory prior to the transfer of the personal information, and the adequate level of data protection shall be guaranteed. This framework is used as a basis for the APEC Cross-Border Privacy Rules ("CBPR"). The U.S.-led CBPR system comprises Privacy Enforcement Authority, privacy certification institutions and recognized entities operating upon nine general privacy principles and a bundle of practical requirements. A joint APEC-EU working team attempts to discover more opportunities for "double compliance" via EU BCR and APEC CBPR referential[10]. Additionally, the Southern African Development Community (SADC) developed the Model Law on Data Protection in 2010 containing general data protection principles for cross-border data transfer. Notwithstanding the efforts, many African countries are still struggling with enacting laws to regulate the collecting and processing of personal information. The organisations' practices stopped at proposing a broad framework of guidance. Further discussions over effective solutions to the conflicts of applicable laws of personal data transborder regulation are needed. However, the international negotiations and corporations are worthy of recognition.

1.2. Problem Statement

China is imminently in need for a strong and more coherent data transborder flow regulatory framework, backed by transparent enforcement and legal certainty. As the world's second largest economy, China's demand for data exchange across borders has grown significantly. On one hand, cross-border e-commerce transactions reached 134.7 billion RMB (approximately 17.7 billion Euro) and is expected to reach one trillion Euro by the year 2020, accounting for 37.6% of China's total imports and exports[11]. On the other hand, technical innovations have brought unprecedented threats to privacy and data security. Furthermore, global trade and political tensions are rising. Against this background, China needs to carefully assess domestic and international economic and legal situations to create a quality strategy for cross-border data flow regulation.

China's cross-border data transfer regulation is an evolving project that still under development, with various administrative regulations and department rules mushrooming. The Personal Information Protection Law has been incorporated into the law-making plan of the 13th Standing Committee of National People's Congress, and was released with the draft for public comment on October 21, 2020. The legislators especially emphasised the protection of public interest and state security, taking into account the needs of the protection of data subject's rights, and took a reluctant position on the regulation of cross-border data transfer. *The Cybersecurity Law* (enacted in 2017) for the first time addressed data localisation and security assessment of data export requirement for Critical Information Infrastructure providers[12]. *The Civil Code of China* (adopted May 28, 2020) newly introduced greater protection of privacy rights and personal information[13]. It clarified that (i) the rights and interests of natural persons over their personal information are civil rights and private rights; (ii) the natural persons' rights to their personal information belong to personality rights; and (iii) the distinction is made between privacy and personal information. These three pieces of legislations constitute the foundation of China's personal information protection laws.

The Measures on Personal Information and Important Data Export Security Assessment (draft for comments) was released on 2017 by the Cyberspace Administration of China (CAC). It was planned to contain elements in the scope of the security assessment, such as the consent of data subject, the security protection status of data recipient, and risk of data leaving China. Upon receiving constructive criticism, the CAC updated its second version of *The Measures on Personal Information Export Security Export* (draft for comments) in 2019. One essential element – the important data – was removed while one important element – the standard contractual clauses – was introduced.

This paper aims to provide a comprehensive analysis of China's cross-border data transfer regulation. The rest of the paper is organised as follows. Section 2 demonstrates how the personal data protections laws have evolved owing to transitions in the Chinese economy with a focus on the objectives and characteristics of cybersecurity law followed by how the Cybersecurity Law (CSL) is enforced and authorities responsible for the same. Section 3 highlights

the Data Export Regulations in China, broadly classified into Critical Information Infrastructure Data Export and Personal Data Export and how the approaches vary in terms of the measures and assessments. This section is followed by the conclusion derived from this study. Notably, this paper includes important drafts of laws and regulations to demonstrate the possible future developments in China.

2. The Evolution of China's Personal Data Protection Laws

Chinese concepts of privacy and personal data protection vary through different historical periods. Most of them are rooted from Chinese traditional ethics or moral standards, and partially integrated with socialism ideology[14]. Since the economic transmission from central planned market to free market in the 1990s, Chinese communities began to experience greater variety of roles in participating economic, societal and political activities. Although traditional predominant values still hold a deep influence on people's behaviours, individualism and subjectivity have dramatically been promoted in their social life. Scrutiny and concerns over the importance of individual's privacy and protection of emerging personal data processing are ever growing. Baidu, the largest Chinese search engine provider, was sued by a consumer rights protection association for illegally collecting user data without consent[15]. Alibaba, another internet giant, was challenged by Chinese users for the misuse of their digital transaction records and social media presence on Zhima Credit (an online credit service that offers loans based on users' digital activities)[16]. The consciousness of privacy in contemporary China has been gradually expanded and individuals have raised their expectations for the right to be let alone.

Prior to the CSL, China's personal data protection policy was integrated in a number of laws and administrative rules through the protection of personal dignity and reputation. Article 28 of the Chinese Constitution provides citizens an inviolable personal dignity from "insult, defamation or false charge." Article 252 of Criminal Law (1997) prohibits any violation to the freedom of citizen's communication rights by hiding, destructing or illegally opening other's letters. Article 101 of General Principles of Civil Law (1986) confers natural person and legal person the right of reputation. The Supreme People's Court in 2001 for the first time confirmed the legal ground for claiming remedies for the damages caused by the violation of one's privacy or other personal rights.

Personal Information was firstly defined in the Notice concerning Punishing Criminal Activities of Infringement of Citizen's Personal Information in 2013, stating that "personal information includes any information that can identify the citizen's personal identity or information and data involving the citizen's personal privacy, such as name, age, ID number, and so on." In response to the rapid development of technology, Chinese authorities released over 200 pieces of laws, administrative regulations and sector-specific rules regulating the collecting and processing of personal information across domains like banking, healthcare, medical record or disease control[17]. A comprehensive framework for personal data protection laws is urgently in need.

2.1. Cybersecurity Law

In November 2016, the final legislation of Cybersecurity Law was passed by the Standing Committee of National People's Congress imposing new cybersecurity requirements on *network operators* that "own or manage networks, or provide network services." It applies to any activities related to the "construction, administration, maintenance and use of networks."[18] The CSL is up to date the highest-level legal instrument concerning personal information protection in China. Be broad as it is, three pillars constitute the substantive provisions of the Law: multi-level protection scheme, critical information infrastructure protection, and personal information protection.

2.1.1. Objectives

Article 1 of the CSL sets multiple objectives aiming to "safeguard cyberspace security, to guarantee cyberspace sovereignty, state security and social public interests, to protect legitimate interests of citizens, legal persons and other organisations, to promote the health development of informationalisation of economic society"[19]. This is aligned with the special aspect in terms of multiple objectives in Chinese law makings, particularly those areas where face most of the challenges brought by emerging issues. As this provision suggests, the objectives are to govern everything within the country's cyberspace infrastructure, ranging from internet activities to data export.

The downside is, however, observable. It is not unusual that such generality and flexibility, sometimes excessive omissions, can be found in Chinese law drafting. Coupled with a wide discretionary power conferred on lower-level competent authorities in order to implement the law, predictability and certainty of law often are compromised. Furthermore, in order to identify a complete set of independent objectives and to prioritize them, the law makers are re-

quired to hold clear concepts, logical foundations and thought-provoking procedures[20]. In China, most of the data protection rules were made in the response to an existing problem. Despite insufficient experiences in data protection law makings and "rent-seeking" among various authorities, one essential aspect is the missing of a unified value for the protection of personal information. It is yet not crystal clear in other jurisdictions as technology and law in this regime are significantly inter-dependent. Without the clear value set ahead, multiple objectives would affect the fundamental principles as well as the conceptual framework of data protection. The immediate consequence is the vague defining of rights and obligations for stakeholders involved. This echoes the lack of legal predictability and certainty.

2.1.2. Multi-level Protection Scheme

Article 21 of the CSL requires all network operators to be obliged with different security measures according to the *cyberspace Multi-level Protection Scheme* (MLPS). Under the MLPS, network operators shall safeguard the cyberspace from interference, destruction or unauthorised access, and to protect the internet data from leak or fraud. Security obligations include but not limited to (i) the establishment of the internal security management protocol; (ii) the appointment of a person in charge of security affairs; (iii) the deployment of technical measures for cyber attacks; (iv) the record of internet operation activities no shorter than six months and the response plan for security incidence; and (v) the classification of data and the backup and encryption of the important data.

The MLPS was born from the demands of the national computer system security in 1994 and thus falls under the competence scope of the Ministry of Public Security (MPS). After a series development of administrative regulations, the updated draft of *Regulation on Cybersecurity Multi-level Protection Scheme* as a milestone was released in 2018. Together with a bundle of supplementary national technical standards, the so-called MLPS 2.0 framework of cybersecurity in China is finalised[21]. The MLPS Regulation as a supporting document of Article 21 CSL defines descriptive obligations and requirements for the network operators fell under different levels of MLPS. Eleven general obligations are listed to clearly allocate the liability and to set technical and organizational security measures. Specific obligations need to be met according to the level of the network operator's activities that would affect the state and public security, scaled from 1 the least risky to 5 the most risky[22]. After being classified, which is based upon a self-assessment, the network operators are required to deploy special security measures such as personnel management, datasets backup and encryption to protect important data.

The compliance with the MLPS 2.0 will be essential for understanding the personal data export regulation in China. Not only because such compliance is mandatory, but also the second pillar of the CSL, critical information infrastructure protection, is based on the classification within MLPS.

2.1.3. Critical Information Infrastructure

Critical Information Infrastructure (CII) is a major challenge in implementing China's cybersecurity strategy and had been recurred at top-level national cybersecurity meetings. On the basis of the cybersecurity MLPS, the state implements key protections to CII which, «if destroyed, suffering a loss of function, or experiencing leakage of data, might seriously damage national security, social welfare, and public interests.» A non-exhaustive example list (including public telecommunication and information service, energy, transportation, water resources, finance, public service and e-governmental information) is given in Article 31 CSL showing the broad scope of the application of CII requirement. In principle, any network operators that being graded above level III (including level III) under the MLPS shall be regarded as CII operators.

CII operators are imposed stricter security requirements due to the nature of the data being processed. More importantly, Article 37 CSL rules that:

«Personal information or important data that CII operator collected or generated during its operations within the territory of the People's Republic of China shall be stored within the territory of China.»

Transferring CII information outside of China is only allowed under exceptional circumstances where actual needs for business are in place and a security assessment is approved by competent authorities. Under the CSL, CII operator is the only subject-matter that is required to comply with the data localisation policy and security assessment for cross-border data transfer. However, the definitions of CII and other key concepts such as important data remain unclear.

CII is in essence a network facility, information system, digital asset, or a collection of such elements[23]. In the early stages of informationalisation, CII was considered to be part of Critical Information (CI) that was scoped clearly. With the changing of the technical landscape, sources of risks are far beyond the scope of CI, such as the attacks coming from

virtual entities, i.e. ICT or Operation Technology domain[24]. At present, large-scale network destruction of CII is a high-risk yet low-probability incident that very limited examples of CII being damaged from cyber-attacks or data leakage can be provided. Therefore, the assessment of security and risks of CII mainly reply on the experts in the domain, instead of evidences or case studies. This brought inconsistency in determining the scope of CII and eventually made it difficult to implement relevant policies. Generally, all ICT service providers fall within the scope of CII operators according to the laws, which is not efficient in the digital economic community.

2.1.4. Personal Information Protection

There is no chapter entitled "personal information protection" in the CSL, yet provisions related to the protection of personal information are scattered through this law. Chapter 4 Network Information Security covered most of the personal information protection provisions. Network operator is the core subject-matter that most of the obligations imposed upon. Data subject's rights have been conferred passively through the legal obligations for network operators, i.e. network operator shall correct or delete on the request of the data subject when the personal information are incorrect or wrongly processed.

The structure comprises basic principles for processing, legal grounds for processing and a non-exhaustive example list of prohibited conduct. Personal information can only be collected when data subject is informed and agree to the purpose and scope of the collection. The processing of personal information must follow basic principles listed in Articles 40-42, 47, 49 which share substantive similarities with the APEC privacy framework. Consent is the ONLY legal ground for processing of the personal information[25]. This is to ensure that data subject has sufficient autonomy to decide the way his or her personal data will be collected, processed and distributed. Such autonomy is endorsed by the sufficient informing requirement, meaning that only after data subject is informed of the purpose, scope and means of processing of the personal data can he or she be capable of giving the genuine consent. The network operator has to perform the information obligation before collecting the individual's personal data.

2.2. Enforcement and Authorities

The CSL's provisions relating to data privacy formed the most comprehensive and broadly applicable set of privacy rules. It acts as an umbrella that covers a bundle of administrative regulations and numerous normative texts scattered across most of the industries. To date there is no independent authority for data protection. Multiple competent authorities or supervisory authorities are in charge of the implementation and enforcement of the rules.

2.2.1. Regulatory Framework

Various types of documents have the force of law in China. Among all the legal instruments, the Constitution Law enjoys the highest primacy yet is rarely applied directly. The law made by the National People's Congress or the Standing Committee of NPC has the highest legal effect in the respective regime, such as the Cybersecurity Law.

Administrative regulations are rules promulgated by the State Council. Its legal effect is lower than the Law but higher than the Department rules. To date, two administrative regulations were issued: the *Regulation on Critical Information Infrastructure Security Protection and the Regulation on Cybersecurity Multi-level Protection Scheme*. Additionally, sector-specific administrative regulations also affect China's personal data export study, such as the *Regulation on Computer Information Security Protection and the Regulation on Human Genetic Resources Information Management*.

Department Rules are legal documents issued by the ministries and commissions under the State Council, along with other agencies with administrative functions directly under the State Council. The applicable scope is determined by the competence of the issuing government department. For example, the aforementioned *Measures on Personal Information Export Security Assessment* is a department rule issued by the CAC. To date, around 30 department rules were issued by various authorities in the field of security, data protection and export.

Judicial interpretations are the explanations to specific legal questions made by the State Supreme judicial institutions during the application of the laws. Both the Supreme People's Court and the Supreme People's Procuratorate had released interpretations relating to cases that infringe personal information.

Standards (no legal effect) are mandatory or voluntary technical standards published by the Standardisation Association of China (SAC). In Cybersecurity and Data protection fields, TC260 group under the SAC is responsible for a series of standards titled Information Security Technology that covers methodologies, definitions or scopes of the norms. Within China, national standards play an important role in implementing laws and regulations. Despite the non-compulsory nature, they are better understood as a quasi-regulation rather than a technical specification typically presented in Western context.

Since 2010, over 240 national standards in this field have been published. It is remained debatable with the necessity of such a big amount of technical standards in force.

Additionally, local regulations are directly applied within the scope of the provinces, autonomous regions and municipalities directly under the Central Government.

2.2.2. Competent Authorities

Under the CSL, different parties are in charge of specific area of works. The *State* is to (i) make cybersecurity strategies; (ii) clarify fundamental requirements and objectives of cybersecurity; (iii) guide key area cybersecurity policies and measures. Additionally, the State shall adopt measures to guarantee the cyberspace free from attacks, interferences and crimes. The *network-related industrial associations* shall provide guidance for entities' self-regulation and promote the healthy development of the industries. The *network operators* are required to fulfil obligations addressed in the CSL and to uphold societal responsibilities.

Respectively, the *Congress* is responsible for determining the scope of CII and key areas. The *Cyberspace Administration of China*, an administrative agency directly under the State Council, is in charge of the coordination and management of all cybersecurity related issues. The MIIT and MPS are responsible for supervising and managing affairs within the scope of their competence[26]. The SAC publishes national and sectoral technical standards.

The CAC, also framed as an agency directly under the Chinese Communist Party, inherently carries a heavy stroke of political colour. It is the most important supervisory authority of cybersecurity and directly reports to the State Council for managing Internet information and contents. It works independently from the Ministries of information, public security or commerce. The CAC also leads the drafting of department rules implementing the CSL. Its branches at the province level are the main enforcement institutions that supervise, investigate, and impose administrative fines.

2.2.3. Enforcement

Enforcement of the CSL and related rules in China follows a typical bottom-top approach. Supervisory authorities have broad discretionary powers as well as the competence to impose administrative fines upon entities. Overlapping areas of jurisdictions often pop up among different authorities. The CAC is responsible to coordinate all issues arise through the enforcement. Although not legally binding, the competent authorities often refer to the Information Security Technology standards when performing assessments or issuing certifications.

The supervisory authorities are actively performing their duties since the year 2015. Means of enforcement include communication with the operator, supervising the modification of business, or administrative fines and termination of the operation. A special operation targeting at illegally collecting and processing personal information through mobile applications is jointly conducted by the CAC, MIIT (Ministry of Industry and Information Technology of the People's Republic of China) and SPS.

It is rebuttable that the CAC has the competence in imposing administrative fines. According to the Organic Law of the State Council, the CAC is not one of the departments under the State Council. The legal ground for the CAC should be Article 11 of the Organic Law of the State Council ruling that "the State Council can establish agencies directly under the Council for managing specific affairs or assisting the Primer to handle specific affairs". However, it is not explicitly informed that which agency the CAC is established for. The official documents issued by the later agencies are categorised as "other kind of administrative documents" which cannot be enforced as the basis for administrative fines[27].

According to the CSL, it is clear that the responsibilities of the CAC is coordination and supervision. Therefore, the rules and measures issued for imposing fines might not be legitimate, even their legal effect could be challenged (emphasis mine). Such gap originated from the boost of cybersecurity legislations, and shall be bridged in the future law makings. With the working-in-progress Personal Information Protection Law, the CAC is expected to (i) remain as an agency under the CCP for supervising the Internet affairs, and the national independent Data Protection Authority is formed for data protection regulation; or (ii) be conferred the legitimacy under the new law.

3. Data Export Regulations

3.1. Critical Information Infrastructure Data Export

The starting point for the study of personal data export is to define the CII operator. Quoting the data localisation requirement discussed in 2.2.3, any personal information or important data that are involved in CII shall not be transferred abroad unless a security assessment is conducted with the supervisory authorities' approval.

Defining CII

On 11 July 2017, the CAC released the draft for comments *Regulation on Critical Information Infrastructure Security Protection* (CII Regulation). Aligned with the CSL, the scope of the CII shall be determined by a two-step test: (i) if business falls within the industry or sector listed in the Regulation; and (ii) if the business is graded security level 3 or above as demonstrated in Table 1.

Table 1: Security levels under the Regulation on Cybersecurity Multi-level Protection Scheme

Subject-matter of the infringement	Severity of damage		
	Harm	Serious Harm	Particularly serious harm
Legitimate interests of citizens, legal persons or other organisations	I	II	III
Social order and/or public interest	II	III	IV
State security	III	IV	V

Additionally, the CAC's Guidelines on State Cybersecurity Inspection (no legal effect) proposed three aspects to help self-evaluating the CII:

1. key business domain, e.g., data centre cloud service, domain name resolution service, or voice data internet basic network and hub in Telecommunication sector;
2. information system or industrial control system that supports the key business, e.g., generator set control system or information management system;
3. quantity of CII device, e.g., registered users above 10 million, or active users above 1 million, or daily transaction exceeds 10 million RMB for a platform service.

Defining CII operator

The rules apply to registered entities operating inside the territory of the PRC, as well as those which do not register inside China but offer business and services to Chinese customers. The criteria to determine whether the entity provides business or service in China include: (i) using RMB as currency; (ii) using Chinese as the language; and (iii) delivering goods to China. Any of the abovementioned criteria is sufficient to lead multinational companies to store the collected personal information and important data inside China.

3.2. Personal Information Export

3.2.1. Personal Information

Personal Information is defined as "any information that is recorded, electronically or by other means, can be used or in combination with other information to identify the identity of a natural person" (Art. 76(5) CSL; Art. 4 Personal Information Protection Law (draft)). It is a commonly adopted "capacity to identity" methodology.

In the Information Security Technology – Personal Information Security Specification 2017, based on the definition given in the CSL, this standard enlarged the scope by using a very expansive wording: "any information recorded electronically or by other means". This targets all operators from both public and private sector, as well as all collecting and processing activities of personal data they conduct. Furthermore, the standard added that "personal information is ... or any information that can reflect a specific natural person's activities". This may be consistent with the broad interpretation of personal data held by the CJEU.

Important Data has been repeatedly addressed in the CSL. It is of crucial importance for assessing CII and CII data export requirement, yet surprisingly not defined in the law. The draft of Information Security Technology – Data Export Security Assessment Guidelines (the Guidelines) defines important data as "raw data and inferred data collected or generated by entities, organisations and individuals inside of China, that do not involve national secrecy, but are closely related to state security, economic development or public interests". Publicly accessible government information is excluded from the scope of important data. An index for determining important data is attached with this standard, comprising of 27 main categories and 223 sub-categories. The categorisation is similar to the U.S. Controlled Unclassified Information (CUI) system.

3.2.2. Measures on Personal Information and Important Data Export Security Assessment 2017

On 11 April 2017, the CAC circulated the draft for public comments entitled "Measures on Personal Information and Important Data Export Security Assessment" (the 2017 Measures). Unlike the CSL, the 2017 Measures expand the subject-matter of Article 37 CSL from "CII providers" to "network operators". Under the CSL, any owners or managers of networks and network service providers are defined as network operators. It is disappointing since the main issue

that practitioners were expecting from the 2017 Measures is to distinguish between the CII operator and the ordinary network operators. A clear definition of important data is also missing, only stated that "data closely related to state security, economic development and societal public interests." It further cited the Guidelines as the reference.

Being the first legislation concerning data export regulation of China, the 2017 Measures provided guidance to assess the necessity of the export and data that are prohibited from exporting. Security assessment is classified into self-conducted and authority conducted. Data that do not exceed the benchmark (500,000 pieces of personal information/1,000 GB data/important domains) can be exempted from administrative procedures of approval. Unfortunately, all essential issues were kept untouched, or otherwise worded vaguely, making it very difficult to comment.

3.2.3. Measures on Personal Information Export Security Assessment 2019

After receiving a large number of public comments, the CAC published the second draft titled "Measures on Personal Information Export Security Assessment" (the 2019 Measures). As its name suggests, the 2019 Measures only apply to personal information. The legal requirements set out in the 2019 Measures are significantly more onerous than the 2017 Measures. Within two-year considerations, the legislators demonstrated observable preference in data export regulation approach.

Data localisation

The 2019 Measures require all personal information to be stored domestically for security assessment before being provided to recipients outside of China[28]. Two aspects are implied: all personal information need to be locally stored; and all personal information exports need to go through security assessment.

While data localisation is gradually adopted in international data regulation standards, one shall notice that data localisation does not necessarily mean the restrictions over cross-border data flows. Either the EU GDPR or the U.S. CUI system both emphasise that data localisation, backed with transparent regulatory rules, can reconcile the objectives of safeguard state security and personal rights and free flow of data across borders, which are of equal importance. The 2019 Measures itself aims to functioning as a precise and predictable mechanism for cross-border personal data transfer.

Security assessment

Network operators shall submit the applications for a clearance for the personal information export to the province-level Cyberspace Administrations after a transfer contract is signed with the recipient. The supervisory authority after received the application shall conduct security assessment based on the submitted documents, and to complete it within 15 working days, with the possibility of extensions depending on the complexity of the export.

The security assessment focuses on (i) legal compliance; (ii) protection of data subject's rights; (iii) enforceability of the transfer contract; and (iv) the recipient's record on whether it had infringed data subject's rights or had security incidence. When serious data leakage or data misuses occur, the data subjects are unable to protect their legitimate interests, or the parties are unable to provide protection of the personal information, the authority can request the network operator to pause or terminate the transfer. The security assessment shall be performed at least once per two years. When the substantive factors, such as the purpose of transfer or the retention period, have changed, a new application of assessment shall be submitted.

Standard contractual clauses

The requirement of the legally-binding contractual agreement between the network operator and the recipient is probably the biggest surprise in the 2019 Measures. This so-called transfer contract is the EU Standard Contractual Clauses alike, taking into consideration the limitation of territorial jurisdiction, recognises *inter partes* autonomy.

The contractual clauses are required to include: (i) the purpose, type and retention period of the personal information export; (ii) the data subject is the beneficiary of the clauses involving data subject's interests; (iii) the legal ground for the data subject to claim for remedies when infringement occurs; (iv) when the recipient is unable to perform the contract due to its state's legal environment changed, the contract shall be terminated or re-assessed; and (v) the termination of the contract shall not exempt the obligations involving the legislative interests of the data subject, unless the personal information is destroyed or anonymised. The 2019 Measures further clarifies the contractual obligations of network operator and recipient, respectively.

The adoption of standard contractual clauses integrates the regulatory requirements into contract autonomy. It is expected to indirectly abide offshore entities by the China's standard. This approach largely depends on the supervision of the

post-transfer performance of the parties. Considering that China is still waiting for her own Personal Information Protection Law, it is more likely that China's personal data protection and cross-border transfer regulation will be tilted towards the European standard. On the other hand, there is no clear line between personal information and important data. Important data naturally could contain a large amount of personal information. The regulation on important data and important data export is waiting for the other boot to drop.

3.2.4. Personal Information Protection Law (draft)

On 21 October 2020 the Legislative Affairs Commission of the Standing Committee of the National People's Congress released the draft of Personal Information Protection Law (the PIPL) and invited for public comments. Different from the 2019 Measures, the PIPL draft does not require all kinds of personal information transborder activities to be examined through the security assessment.

Derogations

Cross-border transfer of personal information is by default not allowed, unless at least one of the derogations is granted:

1. Where the amount of personal information being processed reaches the threshold for CAC security assessment, the personal information processor shall firstly store the personal information inside China. Such personal information can only be transferred outside of China after the security assessment being conducted and approved by the CAC[29].
2. Prior to the cross-border transfer, the processor shall provide the data subject with information including the identify and contact of the recipient, purpose and means of processing, types of personal information, and means for data subject to implement the rights. The transfer is allowed when the individual's consent is obtained[30].
3. A personal information protection certificate issued by a CAC-recognised organisation[31].
4. Contractual obligations over the recipient with regard to the personal information protection[32] (similar to the contractual clauses described in Sec. 3.2.2).

Restrictions

For the concerns of the protection of China's data subjects and data sovereignty in the global data governance, as well as to achieve a delicate balance in international relations, the PIPL draft for the first time introduced restrictions and countermeasure clauses over personal data. The measures embodied a "black list", on which the subjects to the restrictions or countermeasures will be included in the list that personal information transfer is restricted or prohibited. The applicable conditions of restrictions and countermeasures have also been strictly limited. The subjects to the restrictions include foreign institutions or individuals engaged in personal information processing activities that (i) damage the rights of Chinese data subjects; and (ii) endanger China's national security and public interests[33]. The subjects to the countermeasures are countries or regions that impose discriminatory restrictions, prohibitions or similar measures on China[34].

DPIA requirement

Data protection impact assessment (DPIA) is one of the most important means for the continuous and autonomous operation of the compliance operations that personal information processors shall demonstrate and/or self-certify. Prior to the Personal Information Protection Law, DPIA is recommended via non-mandatory technic standards. For the first time DPIA is ruled as a legal compliance that more stringent requirements have been put forward for the establishment of an organisation's internal compliance system. Specifically, the DPIA is required when personal information are transferred to a recipient that is located outside of China. A period of minimum three years has been proposed as the retention time for keeping the result of the DPIA and the record of the processing[35].

Transfer by national agencies

The access and transfer of personal information are possible based on the request for international judicial assistance. Where national agencies need to transfer personal information abroad, special laws and regulations shall be complied with[36].

4. Conclusion

With the increasing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being broken and reshaped. It is particularly important for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules.

China keeps leveraging the data sovereignty to fasten the law makings to support the develop-

ment of critical technology in digital domains and the infrastructure construction. The cross-border data transfer regulation prefers a strict unidirectional data flow administration that focuses on controlling the flow of the data being transferred outside of China. The regulation is largely orientated by the CAC agencies, which weakens the autonomy for individuals and entities in terms of self-governance and enforcement. It is better to objectively value the importance of efficiency in digital economy and to avoid the excessive rigid adherence to traditional sovereignty, of which, the data localisation requirement as the strongest manifestation of data sovereignty is imposed.

In practice, either the "common European data space" proposed by the European Data Strategy, or the "certified governments" recognized by APEC CBPR system are both an attempt to establish cross-border judicial corporation frameworks among trusted entities for the application of rules and efficient enforcement. However, China has not established a mutual trusted mechanism for transborder data flow with other countries. The proposed initiatives largely remain at the conceptual level without practical operability.

Despite the limitations, there are various positive dynamic developments in the framing of China's cross-border data regulation. The CSL, together with Civil Code and Personal Information Protection Law demonstrate great willingness towards a stronger data protection regime and more flexible regulatory mechanism. By introducing contractual obligations and statutory derogations while strengthening domestic personal data protection standard, it is observable that China's legislation is continually moving towards the European approach. Given the fact that countries are unlikely to form a corporation framework in a short period, cross-border data transfer between China and the EU would be profoundly rooted in bilateral and multilateral trade and investment negotiations.

Notes

[1]There is a lack of clarity as to the meaning of the term "cross-border data transfer" even inside one jurisdiction, and often regulatory instruments use different definitions to apply the measures. The EU General Data Protection Regulation (GDPR) refers to "transfer to a third country of personal data" (recital 153) without defining "data transfer"; the APEC Privacy Framework variously uses the terms "international transfer", "information flows across borders", cross-border information flow" and "cross-border data transfer" interchangeably to refer to the movement of personal data across national borders. The OECD Privacy Guidelines refer to "transborder data flows", defining the term as "movements of personal data across national borders" (Section 1(c)), while the Convention 108 refers to "transborder flows of personal data", defined as "the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed" (Article 12(1)). It is also unclear whether merely making personal data accessible should be considered to result in such a transfer, or whether this requires some active or automatic transmission of the data (see Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971). In this article, cross-border data flow and transborder data flow are interchangeable, based on the context as well as the specific document it is referred to.

[2]See OECD, *Declaration on Transborder Data Flows*, 1985.

[3]See Council of Europe, *Details of Treaty No.108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1985.

[4]See Council of Europe, *Details of Treaty No.181. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, 2004.

[5]Limited signatory countries, overbroad content and free applicable scope eliminate the practical performance of the Convention 108. Additionally, International Law Commission listed "protection of personal data in the transborder flow of information" in its long-term working programs as early as 2006, yet fruitless so far. See *Report of the International Law Commission Fifty-eighth session (1 May-9 June and 3 July-11August 2006)*, p. 489.

[6]The CJEU found that the U.S. government permitted generalized access to electronic information and failed to provide redress mechanisms. Therefore, the CJEU determined that the U.S. law did not provide an adequate level of protection essentially equivalent to EU laws. See *Schrems v. Data Protection Commissioner*.

[7] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM/2015/0566 final.

[8]Digital Rights Ireland brought the first challenge on 2016, seeking the annulment of the determination on the basis that the Shield failed to provide sufficient substantive changes from the Safe Harbor Framework. This challenge was dismissed for lack of admissibility. French advocacy group La Quadrature du Net also challenged the Commission's decision arguing that the Shield not only continues to violate the Charter, but also fails to provide effective redress mechanisms. This case remains pending.

[9]Similarly, the U.S. also reached Swiss-U.S. Privacy Shield Framework with Switzerland.

[10] The Referential for Requirements for Binding Corporate Rules (BCR) and APEC Cross Border Privacy Rules system serves as an informal checklist for companies to apply certifications under the BCR and CBPR system. The referential outlines common compliance requirements and ad hoc requirements for each of the systems. Although the referential was superseded after the enactment of the GDPR in 2018, EU representatives have continued to express a strong interest in developing a work plan for future efforts. See Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents.

[11]See Ministry of Commerce of PRC, *Report on E-Commerce in China*, 2018.

[12]The *Cybersecurity Law*, 2017.

[13]«The personal information of a natural person shall be protected by law. Any organization or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. Any illegal collection, usage, processing, and transfer of the individual's personal information, or illegal trade, making available or disclosure of other's personal information is the violation of law.» Article 111 Civil Code of the People's Republic of China.

[14]See B.S. McDougall, A. Hanson (eds.), *Chinese Concepts of Privacy*, Brill, 2002, p. 8.

[15]See M. Jing, *China consumer group accuses Baidu of snooping on users of its smartphone apps*, 2018.

[16]See X. Wang, *Zhima Credit apologizes for its annual report's "mistake"*, 2018.

[17]China provides direct protection of personal information through The Seventh Amendment of Criminal Law, Tort Law, Telecommunication Law, Junior Protection Law, Consumer Protection Law, etc. Indirect protection of personal information is provided though Constitution Law and Civil Law. For example, the Ministry of Industry and Information Technology is in charge of regulating the ISPs via *Measures on Protecting Personal Information of Telecommunication and Internet Users, Measures on SMS service management*, etc.

[18]*Cybersecurity Law* (n12), Article 2.

[19]*Ivi*, Article 1.

[20]See R.L. Keeney, *Identifying, prioritizing, and using multiple objectives*, in "EURO J Decis Process", 2013, n. 1, p. 45-67.

[21]The three newly released national standards are: (1) GB/T 22239-2019 *Information Security Technology-Basic Requirements for the Multi-level Protection*, (2) GB/T 25070-2019 *Information Security Technology- Cybersecurity Multi-level Protection Security Design Technical Requirements*, and (3) GB/T 28448-2019 *Information Security Technology-Cybersecurity Multi-level Protection Assessment Requirements*, which was into force on 1 December 2019. Another national standard titled GB/T 25058-2019 *Information Security Technology-Implementation Guide for Cybersecurity Classified Protection* comes into effect on 1 March 2020.

[22]For the description of the security levels, see Table 1.

[23]CAC, *National Cyberspace Security Strategy*, 2016 (unofficial English translation). See also, Title VII, the USA PATRIOT Act, 2001; M.P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, National Institute of Standards and Technology of the U.S., 2018.

[24]For example, some malware target industrial operation system in electricity, gas, or chemical plants, while some cyber attacks target the control or tampering of information and data.

[25]*Cybersecurity Law* (n12), Article 41.

[26]*Ivi*, Article 8.

[27]*Law of the People's Republic of China on Administrative Penalty*, 2018, Article 14.

[28]*2019 Measures*, Article 2.

[29]*Personal Information Protection Law* (draft), Article 38(1) and Article 40.

[30]*Ivi*, Article 39.

[31]*Ivi*, Article 38(2).

[32]*Ivi*, Article 38(3).

[33]*Ivi*, Article 42.

[34]*Ivi*, Article 43.

[35]*Ivi*, Article 54.

[36]*Ivi*, Article 41.

* * *

La disciplina cinese del trasferimento transfrontaliero dei dati

Riassunto: In virtù della crescente partecipazione dei paesi emergenti alla governance globale dei dati, il paradigma normativo tradizionale dominato dall'Unione Europea e dagli Stati Uniti viene costantemente disintegrato e rimodellato. È di particolare importanza per la Cina stabilire il quadro normativo del trasferimento transfrontaliero dei dati, poiché non solo coinvolge i diritti dei cittadini e delle istituzioni cinesi, ma anche la sovranità digitale e la sicurezza nazionale, nonché la definizione delle regole globali del cyberspazio. La Cina continua a far leva sulla sovranità dei dati per consolidare i processi di produzione di norme a sostegno dello sviluppo di tecnologie critiche in domini digitali e della costruzione di infrastrutture. Questo articolo mira a fornire una analisi sistematica delle normative cinesi relative allo scambio transfrontaliero dei dati. Vengono analizzate sia le disposizioni già adottate sia quelle in corso di adozione, come anche le norme vincolanti e quelle non vincolanti; vengono inoltre evidenziati gli sviluppi positivi verso la definizione in Cina di un quadro regolatorio del flusso transfrontaliero dei dati. Nonostante alcune limitazioni, la legge sulla sicurezza informatica, insieme al codice civile e alla legge sulla protezione dei dati personali, dimostra un forte orientamento verso un regime di protezione dei dati più forte e un meccanismo di regolamentazione più flessibile.

Parole chiave: Cina – Circolazione transfrontaliera dei dati – Sicurezza informatica

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0027

I profili informatici nella valutazione della responsabilità dell'Hosting Provider

Ciro D'Urso

Il presente contributo ha lo scopo di analizzare i profili tecnico-informatici che emergono, come principali argomenti di indagine, nella valutazione della responsabilità civile dei prestatori di servizi di condivisione online di contenuti forniti dagli utenti (*user-generated contents*). Le riflessioni sono sviluppate con particolare riferimento alla condivisione di contenuti multimediali effettuata senza preventiva autorizzazione del titolare dei diritti di proprietà intellettuale. Si trae spunto dall'osservare che, in ambito nazionale e indipendentemente dalla peculiarità delle singole controversie civili, le questioni tecnico-informatiche che andremo ad esaminare sono state oggetto di approfondimento istruttorio nelle valutazioni del giudice per mezzo di apposite indagini peritali disposte con l'obiettivo di rispondere a quesiti che si riscontrano, con una certa frequenza, sostanzialmente invariati dinanzi a giudici diversi.

Responsabilità civile – Diritto d'autore – ISP - Internet Service Provider – Hosting Provider – Commercio elettronico – Contenuti multimediali

Sommario: *1. Introduzione – 2. Dietro le quinte della normativa: i principali profili informatici – 2.1 La natura attiva o passiva dell'Internet Service Provider – 2.2 Le segnalazioni – 2.3 Gli strumenti – 2.4 Quantificazione del danno – 3. Conclusioni*

1. Introduzione

La disponibilità sulla rete Internet di piattaforme di condivisione di contenuti audiovisivi fruibili online ha attirato l'interesse, a livello mondiale, di centinaia di milioni di utenti, determinando l'affermazione di grandi *player* specializzati (solo per citarne i principali, *YouTube*, *Vimeo*, *Dailymotion*) e di decine di altri siti che, pur erogando in via principale una diversa tipologia di servizio, hanno altresì ampliato l'offerta per consentire ai propri utenti il caricamento e la condivisione di filmati.

Un aspetto fondamentale connesso alla condivisione sui siti specializzati di contenuti caricati da terzi (c.d. utenti) è rappresentato dalla responsabilità civile dei proprietari delle piattaforme tecnologiche tramite le quali avviene l'attività degli utenti. Su questo tema si è assistito negli ultimi anni alla proliferazione di azioni legali, sia in ambito nazionale che europeo, promosse dai titolari dei diritti di proprietà intellettuale delle opere o dei prodotti pubblicati senza autorizzazione nelle suddette piattaforme[1].

Questo contributo analizza i profili tecnico-informatici sottesi alla normativa di riferimento con particolare riguardo alla condivisione di contenuti multimediali effettuata senza autorizzazione dei titolari dei diritti d'autore. Nel corso della disamina verranno anche evidenziati gli aspetti più controversi sui quali non vi è un orientamento giurisprudenziale univoco e, al riguardo, verranno proposti indirizzi di

C. D'Urso è ingegnere informatico e Senior Member dell'IEEE; ha ottenuto la specializzazione con lode in "Ricerca operativa e strategie decisionali" nonché il Master di II livello in "Valutazione delle politiche pubbliche". Docente a contratto presso l'Università LUMSA di Roma, è Consigliere parlamentare del Senato della Repubblica. Le opinioni espresse sono personali e non impegnano in alcun modo le Istituzioni di appartenenza.

indagine tecnico-informatica applicabili ai casi specifici. La sezione conclusiva fornirà l'opportunità di riflettere sulle prospettive future alla luce delle recenti proposte della Commissione europea.

2. Dietro le quinte della normativa: i principali profili informatici

Rinviando ai numerosi e autorevoli contributi della dottrina che analizzano diffusamente la normativa applicabile[2], occorre richiamare per gli scopi del presente lavoro, la direttiva n. 31/2000 ed il corrispondente decreto legislativo di attuazione n. 70/2003. Si farà riferimento, altresì, all'articolo 17 della nuova direttiva sul copyright del Parlamento europeo n. 790/2019 del 17 aprile 2019, ancorché non ancora recepita nell'ordinamento nazionale.

Come noto, la direttiva n. 31/2000, e conseguentemente il decreto legislativo 70/2003 (nel seguito anche rispettivamente "direttiva" e "decreto"), classificano i prestatori[3] di servizi della società dell'informazione[4] (anche detti ISP - Internet Service Provider o Hosting Provider) in tre diverse categorie in base alla tipologia di servizio erogato. In estrema sintesi sono individuati servizi di[5]: semplice trasporto su una rete di comunicazione di informazioni fornite da un destinatario del servizio e fornitura dell'accesso alla rete di comunicazione (*mere conduit*); memorizzazione temporanea di informazioni fornite da un destinatario del servizio allo scopo di rendere più efficace l'inoltro ad altri destinatari (*caching*), memorizzazione non temporanea di informazioni condivise da un destinatario del servizio (*hosting*). Allo stesso tempo, il legislatore configura una disciplina sulla responsabilità dei prestatori per i contenuti illecitamente pubblicati dagli utenti pur escludendo un obbligo di sorveglianza preventivo e generalizzato.

Procediamo, quindi, per gradi e identifichiamo i più rilevanti profili informatici coinvolti nella valutazione della responsabilità dell'Hosting Provider facendoci guidare dalla normativa richiamata.

In particolare, i considerando dal 42 al 48 e gli articoli dal 12 al 15 della direttiva, nonché gli articoli dal 14 al 17 del decreto, delineano i principi in base ai quali valutare la responsabilità dell'ISP, unitamente alla previsione dell'assenza di un obbligo generale di sorveglianza. Nella giurisprudenza nazionale, tuttavia, si è venuta a formare una distinzione che non si rinviene nella citata normativa. Infatti, nelle decisioni dei giudici di merito indicate nella nota 1 si osserva l'evolversi di una ulteriore classificazione introdotta dal giudice tra Hosting Provider attivo (ovvero non neutrale) e passivo (ovvero neutrale) sulla base delle caratteristiche del servizio erogato[6]. Sul punto occorre peraltro evidenziare che l'esenzione della responsabilità di cui all'articolo 16 del decreto non è comunque automaticamente riconosciuta all'ISP cosiddetto passivo[7]. Dunque il primo aspetto che il giudice affronta nelle controversie legali analoghe a quelle citate concerne senz'altro la natura dell'ISP in relazione ai fatti contestati.

Successivamente, chiarito il regime giuridico applicabile in relazione alla determinazione della natura del fornitore, occorre avere riguardo al comportamento tenuto dal medesimo con particolare riferimento al principio del considerando 46 della direttiva: «per godere di una limitazione della responsabilità, il prestatore di un servizio della società dell'informazione consistente nella memorizzazione di informazioni deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite». È interessante notare che analoga previsione si rinviene nella direttiva n. 790/2019 all'articolo 17: «... sono responsabili ... a meno che non dimostrino di ... aver compiuto ... i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti ... e in ogni caso aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento ...». Ecco che emerge l'ulteriore aspetto tecnico recato dagli aggettivi "pertinenti e necessarie" e "sufficientemente motivata": anche in questo caso la giurisprudenza non è univoca. Infatti, alcune sentenze identificano come informazione indispensabile l'indicazione "qualificata, puntuale e circoscritta" dei contenuti contestati per mezzo degli indirizzi URL (vedi *infra*)[8], al contrario, in altre decisioni, il giudice ha ritenuto sufficiente un'indicazione "specifica dei file illeciti con ogni mezzo" (e.g., il nome della trasmissione televisiva o il titolo del film)[9]. Anche in questo caso le argomentazioni tecnico-informatiche possono chiarire al giudice l'eventuale fattibilità ed efficacia della ricerca ed estrapolazione dei contenuti illeciti sulla base di informazioni generiche.

Il prestatore, ricevuta la segnalazione, ha agito tempestivamente? Ovvero, per usare le parole della direttiva n. 790/2019[10]: ha disabilitato l'accesso o rimosso le opere o altri materiali oggetto di segnalazione e ha compiuto i massimi sforzi per impedirne il caricamento in futuro? Dal quesito discendono alcuni aspetti tecnici non privi di complessità anche correlati alle modalità tipiche della segnalazione. Essa

infatti può consistere, come accennato, in una lista di titoli (per esempio, di programmi o film) corrispondenti a file pubblicati illecitamente sul sito contenenti cospicue parti o singole scene dell'opera originaria. Su questa base si dovrebbe ritenere che il provider a partire da questo momento è "informato", ai sensi del considerando 46 della direttiva, delle attività illecite, e che quindi dovrebbe agire con una rimozione *ex-post*[11] dei contenuti esistenti sulla propria piattaforma. Ma, per lo stesso principio di diligenza e tempestività, dovrebbe anche impedire *ex-ante*[12] il caricamento di brani analoghi estratti dall'insieme di opere segnalate. A questo scopo vengono in soccorso due tipologie di strumenti informatici, la prima agisce sia *ex-ante* sia *ex-post*, la seconda invece unicamente *ex-post*.

Il percorso logico fin qui seguito ci conduce infine alla quantificazione del danno, la cui elaborazione necessita di analisi molto approfondite sulle caratteristiche (più propriamente metadati) dei singoli file pubblicati illecitamente nel tempo. L'esame può richiedere il controllo, come avvenuto nel coso di taluni giudizi, di evidenze informatiche risalenti anche a un decennio prima.

2.1. La natura attiva o passiva dell'Internet Service Provider

La sentenza della Suprema Corte di Cassazione del 19 marzo 2019, n. 7708, è intervenuta sul tema della responsabilità dei prestatori di servizi della società dell'informazione (caso RTI v. Yahoo!). La parte convenuta in questo caso non è stata riconosciuta quale provider "attivo", ma la Cassazione ha colto l'occasione per chiarire la distinzione tra Hosting Provider attivo e passivo[13] introducendo tre elementi che influenzerebbero tale classificazione. Ad avviso della Corte, il prestatore di servizi di hosting svolge un ruolo attivo, allorché esso compia una o più delle seguenti operazioni sui contenuti: filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione, promozione (primo elemento: c.d. "indici di interferenza"), se effettuate nel contesto di una gestione imprenditoriale del servizio (secondo elemento). La Corte ha aggiunto, altresì, che anche le tecniche di valutazione comportamentale degli utenti possono avere rilievo nel riconoscimento in capo all'ISP di un ruolo attivo, allorché esse siano impiegate per aumentare la fidelizzazione degli utenti con lo scopo di completare e arricchire, in modo non passivo, la fruizione di contenuti da parte di un pubblico indeterminato (terzo elemento). Conseguentemente, i citati tre elementi sottoposti alla valutazione del giudice dovrebbero essere accertati in corso di causa e, trattandosi di profili molto tecnici, appare indispensabile l'ausilio del consulente d'ufficio che approfondirà gli aspetti che nel seguito andiamo a descrivere.

Gli elementi citati primo e terzo devono essere controllati analizzando il comportamento del sito web rispetto all'interazione con le diverse tipologie di utenti, considerando quantomeno da un lato l'azione di un utente anonimo fruitore di contenuti e dall'altro di un utente produttore dei medesimi e registrato sulla piattaforma. Si applica, in tal caso, un metodo sperimentale avendo riguardo alle funzionalità del sito attivate durante la navigazione anonima e a quelle utilizzate nel corso del processo di caricamento dei file, nonché all'effetto di queste ultime sulla catalogazione e ricerca dei contenuti, considerando, peraltro, anche l'eventuale indicizzazione da parte di motori di ricerca esterni al sito stesso. Un ulteriore aspetto da apprezzare ai fini della valutazione del giudice, che si pone a metà strada tra il secondo e il terzo elemento sopra elencati, è costituito dall'analisi degli eventuali annunci pubblicitari visualizzati durante la navigazione dell'utente, i quali presuppongono una monetizzazione degli accessi al sito stesso e, eventualmente, una profilazione del comportamento[14]. Inoltre, particolare cautela deve essere esercitata nella compilazione delle conclusioni tecniche valutando i risultati ottenuti anche alla luce delle motivazioni del considerando 42 della direttiva, spesso richiamato dalle parti convenute, allorquando stabilisce la sussistenza della deroga alla responsabilità per l'attività di "ordine puramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce, né controlla le informazioni trasmesse o memorizzate". Infatti, con le attuali tecniche di intelligenza artificiale (*machine learning*), i processi automatici che è possibile "programmare", affinché il contenuto degli utenti sia opportunamente elaborato dai calcolatori, sono divenuti particolarmente sofisticati. Basti pensare per esempio ai metodi di riconoscimento e classificazione delle immagini. In altre parole, è vero che operazioni di questo tipo possono essere automatiche (eseguite dal calcolatore), ma è altrettanto vero che gli algoritmi per eseguirle sono predisposti da tecnici informatici che li personalizzano per essere utilizzati nella piattaforma in esame.

Per quanto riguarda il secondo elemento sopra richiamato, risulta sufficiente approfondire il modello di business del fornitore di servizi, segnatamente soffermandosi sulla descrizione del funzionamento dell'organizzazione dal punto di vista dei clienti, dell'offerta, delle infrastrutture e della solidità finanziaria, facendo riferimento agli schemi (*patterns*) rappresen-

tativi dei modelli più diffusi nell'ambito dei servizi della società dell'informazione[15]. In particolare, nel caso delle piattaforme leader di mercato, il carattere *multi-sided* del business è rappresentato quantomeno dal *pattern Freemium*: il servizio di base è gratuito, si paga per avere qualcosa in più.

2.2. Le segnalazioni

I brani audiovisivi pubblicati nelle piattaforme citate sono fisicamente dei file memorizzati in apparati tecnologici controllati dal prestatore di servizi. Essi sono identificati per mezzo di una stringa alfanumerica chiamata URL[16]. Il contenuto di una segnalazione[17] effettuata dal titolare dei diritti e indirizzata al provider può essere così dettagliato da contenere tutte le URL dei file contestati, ovvero un elenco esaustivo dei titoli dei film e delle trasmissioni rivendicate unitamente ad un campione esemplificativo di URL. L'idoneità del contenuto della predetta segnalazione a costituire informazione "pertinente e necessaria" tale da rendere effettivamente edotto il prestatore circa l'illegittimità del contenuto pubblicato è valutata dal giudice in relazione alle risultanze peritali concernenti gli strumenti utilizzabili dal prestatore di cui si dirà nel successivo paragrafo. La Comunicazione della Commissione europea COM(2017)555, del 28 settembre 2017, in merito alle segnalazioni (sezione 3.2.3), consiglia di predisporre «meccanismi efficaci volti a facilitare la presentazione di segnalazioni sufficientemente precise e adeguatamente giustificate al fine di consentire alle piattaforme di prendere decisioni rapide e informate sui provvedimenti da adottare», aggiungendo, rispetto alla forma delle stesse segnalazioni, che esse dovrebbero contenere «una chiara indicazione dell'ubicazione del contenuto potenzialmente illegale (ad esempio l'indirizzo URL)».

L'indirizzo giurisprudenziale, anche in questo caso, non è univoco nell'affermare la necessità di comunicare l'elenco completo degli indirizzi URL. Infatti è possibile citare, ad esempio, le decisioni: Corte d'appello di Milano, n. 29/2015 (RTI/Yahoo!) e Tribunale di Torino n. 1928/17 (cit.), nelle quali è stabilito che si debba «... escludere che una generica diffida, contenente i soli titoli commerciali dei prodotti audiovisivi, sia idonea a far venire meno la neutralità del gestore, e quindi attivare la sua responsabilità»[18]. Di segno opposto, invece, le decisioni: Corte d'appello di Roma, sentenza del 29 aprile 2017 (RTI – Break Media); Tribunale di Roma, ordinanza collegiale del 14 febbraio 2014 (RTI c. Google) e sentenza del 15 luglio 2016 (cit.) e, da ultimo, sentenza del 10 gennaio 2021 (RTI c. Dailymotion) (cit.), nelle quali è stabilito che le informazioni necessarie e sufficienti che il titolare dei diritti deve fornire al gestore di una piattaforma possono consistere in un elenco dei titoli commerciali dei programmi e non necessariamente dei singoli indirizzi URL per la localizzazione dei video contestati[19].

Tra l'altro, è la stessa sentenza della Corte di Cassazione n. 7708 (cit.), a fornire una *ratio* della non univocità delle decisioni di merito, nonché della necessità di esaminare caso per caso la questione in parola, allorquando stabilisce che «l'idoneità della comunicazione al prestatore del servizio a consentire al destinatario la comprensione e l'identificazione dei contenuti illeciti va valutata caso per caso, a tal fine deve allora aversi riguardo ai profili tecnico-informatici per valutare se, nell'ipotesi di trasmissione di prodotti video in violazione dell'altrui diritto di autore, questi siano identificabili mediante la mera indicazione del nome della trasmissione da cui sono tratti e simili elementi descrittivi, oppure occorra anche la precisa indicazione del cd. indirizzo URL». La stessa Corte, tuttavia, con sentenza n. 7709/2019, trattando il caso di un prestatore di servizi della società dell'informazione che esercita la mera attività neutrale di *caching*, stabilendo che la responsabilità prevista dall'articolo 15 del d.lgs. n. 70 sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti – pur essendogli ciò stato intimato dall'ordine proveniente da un'autorità amministrativa o giurisdizionale – ha inoltre aggiunto che, nel caso di specie, la notizia contenuta nella diffida extragiudiziale era generica, in quanto priva delle specifiche indicazioni dei singoli filmati contestati e del loro posizionamento tramite URL. Osserviamo, quindi, che anche in questo contesto l'intervento del consulente tecnico del Giudice risulta dirimente. In particolare esso sarà finalizzato a certificare la natura del prestatore di servizi, sulla base di opportune indagini peritali aventi ad oggetto l'analisi della piattaforma informatica e degli algoritmi utilizzati per erogare il servizio.

Sul punto, inoltre, è utile osservare che una funzionalità, resa disponibile dai siti dei principali prestatori, consiste nella possibilità di inviare puntuali segnalazioni di violazioni, utilizzando una modulistica online per sottomettere la richiesta del cosiddetto *take down*, in linea, tra l'altro, con quanto previsto dal paragrafo 9 dell'articolo 17 della già richiamata direttiva n. 790/2019: «gli Stati membri dispongono che i prestatori di servizi di condivisione di contenuti online istituiscano un meccanismo di reclamo e ricorso celere ed efficace che sia disponibile agli utenti dei loro servizi in caso di controversie in merito alla disabilitazione dell'accesso a – o alla rimozione di – specifiche opere o altri materiali da essi caricati».

Osserviamo che le piattaforme con sede legale negli USA (come Vimeo) nelle predette pagine web fanno riferimento al *Digital Millennium Copyright Act* (DMCA), una legge degli Stati Uniti d'America sul copyright che implementa i due trattati del 1996 dell'Organizzazione Mondiale per la Proprietà Intellettuale. Il DMCA rende illegali la produzione e la divulgazione di tecnologie, strumenti o servizi che possano essere usati per aggirare le misure di accesso ai lavori protetti dal copyright e prevede, altresì, un inasprimento delle pene per la violazione del copyright su Internet. Tipicamente, questa funzionalità è contenuta nella sezione del sito dell'Hosting Provider dedicata all'illustrazione delle linee guida per l'utilizzo corretto del servizio (*Terms of service*).

2.3. Gli strumenti

Affrontiamo in questa sezione la questione concernente le modalità tecniche idonee ad identificare i video pubblicati in violazione dei diritti d'autore. In tale contesto, è utile fare riferimento anche alla Comunicazione della Commissione europea COM(2017)555 (cit.) ove vengono prospettati alcuni orientamenti alla luce del quadro giuridico vigente. In particolare si evidenzia come le piattaforme online, ad oggi, dispongono solitamente dei mezzi tecnici per identificare e rimuovere i contenuti illeciti e che, alla luce del progresso tecnologico nell'elaborazione di informazioni e nell'intelligenza artificiale, l'uso di tecnologie di individuazione e filtraggio automatico sta diventando uno strumento ancora più importante nella lotta contro i contenuti illegali online.

A questo fine, da un punto di vista più tecnico, occorre distinguere due principali modalità: (i) una basata sulla tecnica del c.d. video *fingerprinting*; (ii) l'altra basata su una ricerca per parole chiave almeno parzialmente automatizzata.

Una generica organizzazione che produce contenuti (audio o video) ha interesse a controllare la distribuzione e l'uso degli stessi, al fine di proteggere gli investimenti effettuati. In tale contesto, negli ultimi venti anni, vi è stata una continua evoluzione della tecnologia classificata come *Digital Rights Management* (*DRM*). Si tratta di software sviluppati per aiutare a tenere sotto controllo, in maniera automatizzata, l'utilizzo di contenuti protetti da diritti di proprietà intellettuale. Questa particolare tecnologia è in grado di supportare in modo automatico le seguenti attività: (i) identificazione dei contenuti, (ii) controllo del copyright, (iii) protezione delle copie, (iv) tracciamento degli utilizzi. Le tecniche utilizzate sono varie, a titolo esemplificativo citiamo l'ormai ampiamente diffuso *watermarking*, ovvero l'introduzione nel file video di informazioni aggiuntive che "marchiano", come un tatuaggio digitale, ogni fotogramma. Per gli scopi della presente analisi è, tuttavia, di particolare rilievo la tecnica denominata "video *fingerprinting*". Essa consiste, analogamente a quanto avviene nel caso delle impronte digitali delle persone, nel rilevare alcuni elementi che caratterizzano univocamente il file (video/audio) e nel memorizzarli in una base dati, in modo che sia possibile confrontare successivamente qualsiasi video con le tracce presenti in tale archivio al fine di identificare la presenza di sequenze riconducibili al file originario.

Tale tecnica risponde all'esigenza di rendere disponibile una base dati da utilizzare per identificare una esatta porzione di un contenuto (audio/video) ogni volta che il sistema la incontra, anche in diversi e successivi file. Al contrario, invece, memorizzare l'intero contenuto, per poi utilizzarlo in futuro per il confronto, richiederebbe una quantità di spazio e di capacità elaborativa costosa ed esageratamente grande. Conseguentemente, le tecniche utilizzate sono mutuate dal campionamento statistico, per cui solo un campione del file originario è memorizzato ed utilizzato per operare il confronto. Questo campione rappresenta una sequenza univoca che identifica il file originario e, come nel caso delle impronte digitali, può essere utilizzata per identificare la presenza di quel contenuto in altri file, ma non consente di riprodurre il video o l'audio. Cosa molto importante, con tale tecnica è possibile, con determinati accorgimenti, identificare anche porzioni di audio/video, come per esempio nei video *mash up*, nei quali sono presenti spezzoni provenienti da svariati file opportunamente montati. Dotarsi di un sistema di questo tipo significa implementare innanzitutto un processo al fine di creare l'archivio delle "impronte", e successivamente utilizzare l'archivio così generato per confrontare le "impronte" memorizzate con quelle dei nuovi contenuti audiovisivi. Si osserva, sul punto, che sono disponibili diversi algoritmi di generazione del *fingerprint* dei contenuti audio-video, sia con riferimento alla letteratura scientifica, sia con riferimento a soluzioni di mercato proprietarie o disponibili in modalità "codice aperto" (i.e., *open source*). Tali algoritmi da soli non sono comunque sufficienti, infatti essi devono essere inseriti in un processo tecnico-organizzativo di livello *enterprise* al fine di realizzare i controlli nel contesto di realtà delle dimensioni delle aziende coinvolte nelle cause citate. Si ricorda, peraltro, che la semplice disponibilità di librerie software scaricabili da Internet, previo pagamento di un limitato importo o rese disponibili in modalità *open source*, non determina affatto che un processo di implementazione su vasta scala basato su tali moduli

software sia di per sé "agevole" o "economico" (in particolare la disponibilità di software distribuito in modalità "open source", ancorché non preveda alcun pagamento per la licenza, non implica affatto che il suo utilizzo sia a costo zero, in quanto occorre considerare non solo il costo iniziale ma soprattutto il c.d. TCO - *Total Cost of Ownership*[20]). Si evidenzia, tra l'altro, la presenza di ampia letteratura scientifica sul tema del video *fingerprinting* e della correlata disponibilità di algoritmi e moduli software che li implementano. Basti segnalare che l'elaborazione di tale tecnica risale addirittura al 1983, in particolare fu introdotta, come approccio teorico generale e non specificamente per applicazioni collegate a brani audiovisivi, da un noto articolo di N.R. Wagner[21]. A tale riguardo, è utile fare riferimento, tra gli altri, anche all'interessante illustrazione dell'approccio ai fini del suo utilizzo nelle applicazioni *DRM* che emerge nell'*invited paper* di D. Kundur[22].

Il funzionamento è il seguente: il sistema ispeziona i nuovi caricamenti e i video esistenti per rilevare i casi di uso non legittimo (i.e., video non caricati dal proprietario dei diritti). Il file sospetto viene quindi classificato come candidato per essere oggetto di un'operazione di *take down*. L'utente che lo ha caricato è costretto a rimuovere il video o a cambiare la colonna sonora del video stesso. In alternativa, nel caso l'utente fosse sicuro delle proprie ragioni, il sito consente di sottoporre una richiesta di appello. In relazione ai brani audiovisivi per i quali è stata accertata la violazione di copyright, è possibile utilizzare un metodo di filtro *ex ante* per impedire che brani identici a quelli soggetti a operazione di *take down* siano caricati nuovamente.

Si cita quale esperienza rilevante il caso di Google che ha creato un sofisticato meccanismo per controllare l'uso illegittimo di contenuti audio/video nella piattaforma YouTube. Infatti, la predetta piattaforma consente ai proprietari di contenuti di sottomettere i propri file per elaborarne il relativo *fingerprint* e memorizzarlo nell'archivio appositamente predisposto dalla stessa YouTube. Ogni video aggiunto alla piattaforma è dapprima confrontato con l'archivio centrale delle impronte e solo dopo l'esito negativo della comparazione viene messo a disposizione degli utenti. Tale sistema è noto con il nome di "Content ID". È interessante citare, in questa sede, la collaborazione tra Google e alcuni fornitori di piattaforme software per la gestione automatizzata dei processi relativi al DRM, come per esempio Harmonic Inc. (produttore della tecnologia Rhozet), che prevede la generazione del *fingerprint* compatibile con la piattaforma "Content ID" già in sede di produzione del file audio/video.

Google dichiara[23] che la piattaforma Content ID, usata per la ricerca automatica dei video clip caricati violando il copyright su YouTube, è efficace nel 98% dei casi, solo il 2% dei video privi di autorizzazione richiede la rimozione manuale, inoltre ha reso noto che il giro d'affari del sistema Content ID, usato da YouTube, vale 2 miliardi di dollari. Google ha rivelato anche che gli investimenti nell'antipirateria (in particolare nella piattaforma Content ID) fino al 2015 sono stati pari a 60 milioni di dollari. Per contro, alcune primarie istituzioni che detengono i diritti di importanti opere audio/video non concordano sull'efficacia del sistema di YouTube, dichiarando che esso fallisce nel 40% dei casi, e che, da un certo punto di vista, rischia di legittimare la pirateria[24].

Va osservato che un sistema di questo tipo, se sviluppato in casa, richiede la disponibilità di un'elevata capacità di memorizzazione e di una significativa potenza elaborativa. La realizzazione di una soluzione di questo tipo ha, quindi, costi non trascurabili, sia una tantum (e.g., acquisizione/sviluppo e configurazione/personalizzazione del sistema software), sia ricorrenti (e.g., costi fissi come canoni di manutenzione, retribuzione del personale). Nell'ipotesi alternativa di acquisizione di un servizio da un operatore specializzato[25] i costi sono senz'altro minori rispetto ad una soluzione sviluppata in casa, atteso che l'operatore che offre tali servizi realizza economie di scala in relazione al numero dei clienti posseduti e può spalmare il costo di realizzazione e di manutenzione sul portafoglio clienti. D'altra parte, un servizio di questa specializzazione e con i volumi associati alle piattaforme più diffuse richiede comunque un investimento non trascurabile, che presuppone accordi specifici tra cliente e fornitore, stimabile tra alcune centinaia di migliaia di dollari all'anno e qualche milione (i listini pubblicati dalle aziende specializzate in genere elencano i costi fino ad un numero di video di poche migliaia, per volumi superiori rimandano a specifici accordi presi caso per caso).

Gli strumenti che rientrano nella tipologia fin qui descritta costituiscono, quindi, la tecnica più efficace ed efficiente per il controllo sia preventivo (*ex-ante*, cioè effettuato prima della pubblicazione dei video)[26] sia successivo (*ex-post*, cioè effettuabile anche dopo la pubblicazione dei video) dei contenuti da pubblicare o pubblicati, ed alle cui risultanze subordinare la stessa pubblicazione e/o la permanenza online del contenuto audiovisivo considerato. D'altra parte, se si volesse valutare una modalità tecnica diversa dal video *fingerprinting* utilizzabile *ex-post* (ovvero dopo la pubblicazione del video), si dovrebbe agire facendo uso delle interfacce standard messe a disposizione dalle piattaforme (i.e., interfaccia basata su API -

Application Programming Interface) per interrogare in maniera automatica l'archivio del prestatore di servizi ed ottenere un insieme di video che corrispondono ai criteri di ricerca definiti[27]. Tale modalità certamente non possiede un'efficacia paragonabile al metodo sopra descritto, per contro consente, con un intervento umano successivo all'estrapolazione automatica della lista dei video che corrispondono alla ricerca effettuata, di rilevare un insieme non trascurabile di file da sottoporre al *take down*.

2.4. Quantificazione del danno

In alcune delle sentenze esaminate (citate in nota 1), la quantificazione del danno causato al titolare dei diritti dalla pubblicazione non autorizzata delle proprie opere è avvenuta con riferimento al calcolo delle *royalties*. Con *royalty* si indica il diritto del titolare di un brevetto o di una proprietà intellettuale ad ottenere il versamento di una somma di denaro da parte di chiunque effettui lo sfruttamento dei predetti beni per fini commerciali e/o di lucro. In molti dei citati giudizi, siamo in presenza di opere audiovisive caratterizzate da alti costi di produzione (in termini di mezzi tecnologici utilizzati, risorse umane impiegate e attività organizzative poste in essere) e bassi costi marginali di sfruttamento (a valle della disponibilità del prodotto finale, è possibile replicare l'opera diffondendola mediante svariati canali con un investimento economico molto minore rispetto a quello necessario per produrla). Occorre considerare, quindi, da una parte il titolare dei diritti che, come conseguenza della diffusione non autorizzata delle proprie opere, sperimenta un mancato guadagno derivato dall'impossibilità di sfruttare (e.g., con la pubblicità ovvero con l'eventuale corrispettivo di un abbonamento) i brani audio-video divenuti disponibili su una piattaforma di *video sharing* e fruibili senza controllo da una vasta platea di spettatori. Per contro, la stessa piattaforma di *video sharing* sperimenta un effetto positivo (invero difficilmente quantificabile) in termini di popolarità, maggiori accessi, conseguente aumento di utenti e, eventualmente, maggiori abbonamenti onerosi: in altri termini, il c.d. effetto di rete, su cui però è assai complicato elaborare calcoli adeguatamente motivati.

Ci muoviamo, in base a quanto illustrato, in uno scenario controfattuale per il quale non risulta agevole l'elaborazione di un modello: infatti siamo in presenza di parametri – che definiscono i mancati introiti di una parte e i "guadagni" dell'altra – difficilmente quantificabili. In questo contesto è usuale seguire, per il calcolo del danno, il criterio del prezzo del consenso[28]: conseguentemente, l'individuazione delle *royalties* si sostanzia nella stima dei proventi che il danneggiato avrebbe ottenuto se avesse ceduto a titolo oneroso al danneggiante i diritti di cui quest'ultimo si è invece illecitamente appropriato. A questo scopo l'analisi tecnico-informatica viene espletata avendo riguardo al numero di file contestati, alla loro durata, al tempo di permanenza sulle piattaforme degli Hosting Provider calcolato a far data dalla pubblicazione dei file stessi ovvero dalle segnalazioni del titolare fino alla loro rimozione, al numero di visualizzazioni e *download* nel periodo di disponibilità online.

Occorre, però, ribadire che lo scenario controfattuale in commento è in genere privo di talune informazioni indispensabili per il suo completo svolgimento, le quali non possono essere desunte né dagli atti di causa né da comportamenti passati delle parti. Tale lacuna è determinata principalmente dal fatto che le condizioni di mercato, in particolare la pubblicazione di contenuti multimediali su piattaforma web di condivisione di contenuti per il mercato in lingua italiana, potrebbero non essere rilevabili in precedenti accordi volontari tra le parti o con aziende di produzione televisiva e/o cinematografica per lo sfruttamento di video su una piattaforma web. Una possibilità di approfondimento consiste, in questo contesto, nel provare a sviluppare il calcolo del prezzo del consenso con diverse argomentazioni, tra le quali si citano le seguenti. Una prima argomentazione potrebbe essere basata su contratti stipulati e accordi transattivi sottoscritti in precedenti analoghi procedimenti; un secondo approccio potrebbe essere basato sull'analisi delle modalità con le quali operano quelle aziende che hanno come modello di business la cessione in licenza dei propri contenuti multimediali attraverso acquisti online[29]; la terza potrebbe essere ispirata ai servizi di *Video on demand* messi a disposizione da alcuni fornitori per talune fattispecie di utenti paganti e che consentono agli stessi di ricavare un profitto dalla pubblicazione sulle piattaforme medesime dei brani audiovisivi di propria creazione[30]. Quest'ultima argomentazione si basa sul criterio noto come condivisione del fatturato (*revenue sharing*).

3. Conclusioni

Dalle considerazioni sviluppate, emerge che l'attività del consulente d'ufficio debba proporre al giudice una narrazione che integri i vari aspetti informatici della disciplina applicabile al contesto esaminato, solo apparentemente distinti, presentandoli sotto una prospettiva unitaria e consequenziale. Sulla base dei quesiti posti dal giudice, andrebbe effettuata una disamina delle caratteristiche tecniche che governano le

modalità di erogazione e di fruizione dei servizi, nonché un'analisi delle azioni poste in essere dalle parti, condotta con riferimento alle tecnologie disponibili all'epoca dei fatti. Alcune questioni, come detto, sono ancora in divenire e non univocamente definite in un orientamento giurisprudenziale consolidato, tuttavia occorre anche considerare che ciascun caso fa storia a sé, sia per le caratteristiche dell'Hosting Provider sia per il periodo temporale in cui si collocano i fatti. Probabilmente l'aspetto più controverso delle analisi rimane quello legato alla quantificazione del danno, per il motivo a cui si accennava nel precedente paragrafo, e, cioè, per la difficoltà – che a volte diviene impossibilità – di condurre una motivata analisi controfattuale delle strategie commerciali delle parti.

Volgendo lo sguardo ai possibili scenari futuri e alla possibile evoluzione delle questioni sopra discusse, si segnala che, il 15 dicembre 2020, la Commissione europea ha presentato le proposte di due Regolamenti in ambito digitale: il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA) allo scopo di regolare, sulla base dell'attuale Direttiva sull'e-Commerce (cit.), i cosiddetti servizi digitali. Le due proposte, presentate dalla Commissione, verranno ora sottoposte al vaglio del Parlamento europeo e del Consiglio dell'Unione secondo la procedura legislativa ordinaria.

Con riferimento alla tematica del regime di responsabilità degli intermediari, si osserva, tra l'altro, che la prima delle due proposte, nel mantenere il sistema di responsabilità attualmente in vigore, introduce il principio secondo il quale i meccanismi di *notice and take down* dovranno essere standardizzati, rispettare precisi requisiti e consentire ad ogni individuo o entità di notificare la presenza di specifici contenuti che sono ritenuti illegali. Si segnala, inoltre, l'introduzione di garanzie per gli utenti i cui contenuti sono stati erroneamente cancellati dalle piattaforme e nuovi obblighi per le piattaforme di grandi dimensioni di adottare misure basate sul rischio al fine di prevenire abusi dei loro sistemi.

Parallelamente, il secondo pilastro della proposta di regolamentazione di Bruxelles è quello della concorrenza. Con la legge sui mercati digitali l'Ue interviene sul ruolo dei cosiddetti *gatekeeper*, le piattaforme che hanno una posizione di dominio tale da poter impedire l'accesso di nuove aziende sul mercato, con la previsione di una serie di nuove regole per evitare comportamenti anticompetitivi. Le piattaforme, per esempio, non potranno promuovere i propri servizi a scapito di quelli dei concorrenti e dovranno condividere parte dei loro dati con altre aziende. Sono inoltre previste una serie di sanzioni che possono arrivare fino al 10% del fatturato annuo.

Gli interventi citati, se confermati all'esito della procedura legislativa, consentiranno di proteggere in modo più efficace i diritti fondamentali degli utenti della rete Internet, rendendo i mercati digitali più equi e con minori barriere all'entrata di nuovi operatori. Essi permetteranno, altresì, di rendere più circoscritti gli approfondimenti peritali disposti dal giudice, dovendosi indagare sul rispetto di requisiti tecnici che risulterebbero, almeno in parte, più standardizzati e compiutamente definiti[31] se paragonati a quanto previsto dalla normativa vigente.

Note

[1]Si considerino *ex multis*, in tema di responsabilità dell'Hosting Provider rispetto a contenuti generici forniti dagli utenti: Corte di Giustizia Europea: sentenza 23 marzo 2010, cause riunite da C-236/08 a C-238/08 (Google France c. Louis Vuitton); sentenza 12 luglio 2011, C-324/09, (L'Oréal SA c. eBay International AG); sentenza 16 febbraio 2012, C-360/10 (Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV); sentenza 11 settembre 2014, C-291/13 (Papasavvas c. Fileleftheros); sentenza 14 giugno 2017, C-610/15 (Stichting Brein c. Ziggo BV); Tribunale di Milano: sentenza 7 giugno 2011, n. 7680, RTI c. Italia On Line; sentenza n. 29/2015, RTI c. Yahoo! Italia s.r.l. / Yahoo! Inc; ordinanza 8 maggio 2017, Mediaset c. Live TV; Tribunale di Roma: sentenza n. 17279/2011, RTI c. VBB-COM. Limited/Choopa LLC; sentenza 7 luglio 2016, RTI c. Megavideo LTD; sentenza n. 2883/2017, RTI c. Break Media; sentenza 15 luglio 2016, n. 14279, RTI c. Megavideo (2016); sentenze n. 693/2019, n. 14760/2019, RTI c. Vimeo; sentenza n. 3512/2019, Mediaset c. Facebook; sentenze del 12 luglio 2019, n. 14757, e del 22/01/2021 nella causa RG 62326/2015, RTI c. Dailymotion; Tribunale di Torino: sentenza 1928/17, Delta TV Programs S.r.l c. Google, Inc. / YouTube LLC / Google Ireland Holdings; sentenza n. 342/2018, Dailymotion S.A c. Delta TV Programs srl.

[2]Sulla responsabilità civile degli ISP la letteratura è molto vasta. Si vedano ad esempio: M.R. Allegri, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti*, in "Informatica e diritto, 2017, n. 1-2, pp. 69-112; E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in "Rivista di diritto industriale", 2017, n. 1, pp. 75-122; M. Cocuccio, *La responsabilità civile per fatto illecito dell'Internet Service Provider*, in "Responsabilità civile e previdenza", 2015, n. 4, p. 1312 ss.; G. Sartor, E. Rosati, *Social networks e responsabilità del provider*, Working paper n. 5-Dept. of Law, EUI 2012; M. De Cata, *La responsabilità civile dell'Internet service provider*, Giuffrè, 2010; L. Albertini, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in "Law and Media Working Paper Series 2020", October 7, 2020.

[3]Ai sensi dell'art. 2, c. 1, lett. b), del d.lgs. 70/2003 per "prestatore" si intende: "la persona fisica o giuridica che presta un servizio della società dell'informazione".

[4]Ai sensi dell'art. 2, c. 1, lett. a), del d.lgs. 70/2003 per "servizi della società dell'informazione" si intendono: "le

attività economiche svolte on line, nonché i servizi definiti dall'articolo 1, comma 1, lettera b), della legge 21 giugno 1986, n. 317, e successive modificazioni".

[5]Artt. 13, 14 e 15 della direttiva citata.

[6]Secondo il Tribunale di Roma, tra l'altro, il provider attivo non costituisce una sub-categoria di quello passivo, ma è figura del tutto autonoma che si sottrae dalla disciplina comunitaria e nazionale prevista per l'hosting neutro (sentenza 14757/2019 cit.).

[7]Si veda la recente sentenza del Tribunale di Roma nella causa R.G. 33124/2012, RTI c. Facebook Inc. e Facebook Ireland Limited, nonché il commento: C. Novelli, *Il social giudizioso. La giurisprudenza italiana sulla responsabilità civile degli ISP*, in "Rivista Italiana di Informatica e Diritto", 2019, n. 1, pp. 97-106.

[8]Così Tribunale di Milano, Sentenza n. 29/2015 del 7 gennaio 2015 cit.

[9]In tema di irrilevanza della comunicazione delle URL si vedano le sentenze 14757/2019 e 3512/2019 cit.

[10]Si veda l'articolo 17, sezione 4, lettera c).

[11]Operazione di *take down*: disabilitazione di contenuti pubblicati da un terzo che il titolare consideri in violazione dei propri diritti d'autore.

[12]Operazione di *stay down*: prevenire la ricomparsa di contenuti illeciti analoghi a quelli già oggetto di *take down*.

[13]Si ricorda che la definizione di Hosting Provider attivo" è stata coniata da Trib. Milano, 7 giugno 2011, n. 7680 (cit.): «una diversa figura di prestatore di servizi, non completamente passivo e neutro rispetto all'organizzazione della gestione dei contenuti immessi dagli utenti (c.d. hosting attivo), organizzazione da cui trae anche sostegno finanziario in ragione dello sfruttamento pubblicitario connesso alla presentazione (organizzata) di tali contenuti».

[14]La pubblicità presente sui portali in discorso assume tipicamente tre forme: i) annunci pubblicitari (c.d. "display advertisement"), sotto forma, ad esempio, di banner direttamente visibili sulle pagine; ii) clip pubblicitarie (annunci veri e propri), che l'utente, per fruire del video selezionato, è obbligato a vedere in parte (per es. fino a 15-20 secondi) o per intero (per es. fino a 50 secondi); tali annunci sono riprodotti prima che inizi il video selezionato e/o nel corso della visione dello stesso; iii) banner trasparenti che si giustappongono al video visualizzato, in particolare occupando la porzione inferiore (tali annunci sono simili a banner e possono essere eliminati dall'utente cliccando sull'estremo superiore destro). I predetti annunci pubblicitari generano introiti in due modalità diverse: *pay-per-click* per il primo ed il terzo tipo di pubblicità, *pay-per-view* per la seconda tipologia.

[15]Una pubblicazione di taglio divulgativo, ma non per questo priva di rigore scientifico: A. Osterwalder, Y. Pigneur, *Business Model Generation*, John Wiley & Sons, 2010.

[16]Il World Wide Web (WWW) è uno dei servizi più utilizzati della rete Internet. Esso è realizzato come sistema distribuito client-server, in cui il client è un browser e il server è un server web. Nella comunicazione tra client e server non è sufficiente che richiesta e risposta giungano correttamente al destinatario, occorre che i due programmi comunicanti siano in grado di comprendere le rispettive comunicazioni, cioè "parlino la stessa lingua": devono perciò condividere uno stesso protocollo applicativo. Nel caso del WWW, il protocollo applicativo che specifica il formato della richiesta del browser e della risposta del server web, è denominato "HyperText Transfer Protocol (HTTP)". Per poter accedere ai servizi applicativi messi a disposizione dai server sulla rete è necessario che ognuno di tali servizi risulti univocamente identificabile da parte dei client. Nel caso di Internet è stato definito uno schema uniforme di identificazione applicativa, che consente di assegnare un metodo di accesso e un indirizzo a ogni risorsa presente sulla rete in base ad uno standard chiamato "Uniform Resource Locator (URL)". In generale, una URL ha la seguente forma: protocollo://host:portaTCP/risorsa. Per esempio, nel caso di un video pubblicato su Vimeo.com o su Dailymotion.com: - "https://": rappresenta il protocollo adottato; - "vimeo.com", "dailymotion.com": rappresentano gli indirizzi dei server web a cui è inviata la richiesta; - "367584952", "x7ov2sf": rappresentano il nome del file richiesto, in questo caso l'identificativo numerico univoco di un video pubblicato sui siti corrispondenti.

[17]Tipicamente, con riferimento ai giudizi citati, si tratta di una formale diffida.

[18]Così anche Trib. Roma, ordinanze 22 marzo e 11 luglio 2011, PFA Film s.r.l. c. Google Italia s.r.l. e Yahoo! Italia Inc. (Caso About Elly).

[19]È interessante osservare come nelle decisioni citate questo principio assuma diverse forme: «...la società convenuta poteva facilmente ed autonomamente prendere conoscenza delle violazioni sia per la notorietà dei programmi in questione [...] che, in particolare, per la presenza [...] dei marchi distintivi di RTI»; «...deve disattendersi l'ulteriore censura della necessità dell'indirizzo URL per poter intervenire in modo da rimuovere o impedire in futuro il caricamento dei contenuti lesivi contestati [...] posto che [...] tale dato tecnico non coincide con i contenuti lesivi presenti nella piattaforma»; «...non assume rilievo l'argomentazione difensiva [...] in ordine all'erronea imposizione di un obbligo di controllo preventivo dei contenuti immessi nella piattaforma digitale, in quanto tale obbligo sussiste [...] con riguardo a specifici contenuti [...] una volta avuta conoscenza della natura illecita della diffusione degli stessi»; «... [le diffide] sono idonee a consentire al destinatario di individuare con sufficiente puntualità i singoli contenuti multimediali [...] La responsabilità del provider non può essere esclusa per la circostanza se gli URL [...] gli siano stati indicati o meno».

[20]Si veda, al riguardo, tra l'altro, il breve ma esplicativo intervento di Alfonso Fuggetta.

[21]N. R. Wagner, Fingerprinting, in "Proceedings of the 1983 IEEE Symposium on Security and Privacy", 1983, pp. 18-22.

[22]D. Kundur, K. Karthik, *Video Fingerprinting and Encryption Principles for Digital Rights Management*, in "Proceedings of the IEEE", Vol. 92, No. 6, June 2004.

[23]Cfr. *How Google Fights Piracy 2016 Update*.

[24]BPI-British Phonographic Industry; FIMI-Federazione Industria Musicale Italiana.

[25]Si vedano, a titolo esemplificativo, l'italiana SIAE (siae.it), le statunitensi Nagra-Gudelski Group ex Civolution, Audible Magic, la francese INA.

[26] Al riguardo, M.R. Allegri, *op cit.*, p. 99: «il Tribunale di Torino, nelle ordinanze cautelari relative al caso Delta TV, ha sostenuto non solo l'obbligo per il gestore della piattaforma di rimuovere i contenuti audiovisivi illecitamente diffusi, i cui url erano stati indicati specificamente, ma anche quello di impedire l'ulteriore caricamento sulla piattaforma YouTube dei medesimi materiali, impiegando a tal fine, a propria cura e spese, il software Content ID».

[27]Si pensi a quanto precedentemente detto circa la validità delle segnalazioni di *copyright infringement* prive dell'elenco delle URL ma effettuate con l'indicazione di alcune informazioni relative ai file video, come il titolo, la descrizione, l'autore, i protagonisti, ecc.

[28]Il "prezzo del consenso" corrisponde a uno dei criteri previsti dalla normativa per determinare l'entità del risarcimento dovuto al titolare del diritto da parte dell'utilizzatore responsabile di un illecito sfruttamento dell'opera. Tale criterio è definito dall'art. 158, comma 2, della legge del diritto d'autore che così recita: «Il risarcimento dovuto al danneggiato è liquidato secondo le disposizioni degli articoli 1223, 1226 e 1227 del codice civile. Il lucro cessante è valutato dal giudice

ai sensi dell'articolo 2056, secondo comma, del codice civile, anche tenuto conto degli utili realizzati in violazione del diritto. Il giudice può altresì liquidare il danno in via forfettaria sulla base quanto meno dell'importo dei diritti che avrebbero dovuto essere riconosciuti, qualora l'autore della violazione avesse chiesto al titolare l'autorizzazione per l'utilizzazione del diritto».

[29]Si veda ad esempio: il "Footage Rate Card" della ABC (Australian Broadcasting Corporation); il catalogo della CBC (Canadian Broadcasting Corporation - Archive Sales); il catalogo di Vimeo Stock.

[30]Netflix, Amazon Prime Video, Vimeo On Demand (VOD).

[31]Si veda ad esempio l'articolo 8 del DSA che, con riferimento al contenuto degli ordini emessi dalle autorità giudiziarie o amministrative di contrastare specifici contenuti illegali, menziona tra gli elementi caratterizzanti «[...] uno o più indirizzi URL esatti [...]».

* * *

Digital forensic analysis on the liability of Hosting Providers

Abstract: This paper investigates digital forensic methods related to the assessment of the liability of service providers with respect to user-generated contents. The analysis is developed with particular reference to the sharing of digital video carried out without the prior authorization of the owner. It is inspired by the observation that, at national level and regardless of the peculiarity of the single case, the technical investigation have been the subject of in-depth analysis in the judges' assessments by means of specific forensic analysis concerning some questions that are encountered, with a certain frequency, substantially invariant, in the different judgments.

Keywords: ISP – Hosting Provider – Copyright – Liability – E-commerce – Digital video content

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0031

Il letto di Procuste dei sistemi informativi via Web: un pluralismo falsato?

Alessandra Vernice

Il lavoro contiene una ricognizione di alcune delle principali problematiche legate alla circolazione delle informazioni nell'era digitale. Partendo da una analisi generale dell'architettura costituzionale, prima, e del contenuto del diritto di libertà di informazione attiva e passiva, poi, lo studio si propone di esaminare le differenze fra i nuovi ed i vecchi media, ponendo l'accento sull'assetto dei canali informativi dopo l'avvento di Internet, sui fenomeni informativi che esso ha fatto affiorare, come le fake news e la *filter bubble*, e sul ruolo degli intermediari coinvolti nella ricerca online, quali *search engine* e social network.

Pluralismo – Informazione – Algoritmo – Internet

Sommario: *1. Premessa. Il diritto ad una informazione pluralistica – 2. L'architettura costituzionale e i nuovi media: la convergenza tecnologica – 3. Il nuovo assetto dei canali informativi – 4. Nuovi fenomeni informativi nell'era digitale – 5. Conclusioni*

1. Premessa. Il diritto ad una informazione pluralistica

L'essenza del pluralismo informativo consiste nella circolazione delle diverse idee ed opinioni. Tale diffusione informativa è, strategicamente, una delle condizioni essenziali per il funzionamento dello Stato democratico di derivazione liberale, poiché consente ai cittadini di esercitare la sovranità in modo informato e consapevole[1].

Affinché vi sia una efficace attuazione di tale principio, è necessario, oltre che funzionale, che vi sia il più ampio numero di voci presenti nell'area pubblica di discussione e dibattito e che vi sia il rispetto da parte di tali voci, siano esse pubbliche o private, di regole di indipendenza, obiettività e completezza nell'attività comunicativa, al fine di garantire il diritto, costituzionalmente tutelato, dei cittadini ad essere informati[2].

Se fino a pochi anni fa l'attenzione dei consociati era rivolta soprattutto ai mezzi di comunicazione "ad alta valenza suggestiva", quali la televisione, oggi è necessario considerare tra la pletora dei mezzi comunicativi anche nuove forme di diffusione di contenuti informativi, rese possibili grazie alla esponenziale crescita tecnologica dell'era digitale. Pare quindi opportuno esaminare il forte impatto dei nuovi mezzi di diffusione informativa nelle dinamiche del pluralismo, tra cui, primo fra tutti, l'avvento di Internet.

Infatti, proprio partendo dall'analisi strutturale della Rete delle reti, si può notare che l'automatismo del rapporto di reciproca implicazione tra Internet e pluralismo non è così certo come può apparire ad un primo sguardo. In primo luogo, la mancanza di una regolazione pubblica e l'autoregolazione privata non garantiscono l'imparzialità delle condizioni di accesso e fruizione. Ancora, la deterritorializzazione della Rete, oltre che la personalizzazione algoritmica delle ricerche svolte online, possono potenzialmente favo-

A. Vernice si è laureata presso l'Università degli Studi di Firenze con una tesi in diritto costituzionale. Ha collaborato in vari progetti formativi con l'Università ed il Tribunale Civile di Firenze. Ha conseguito il Master di *Internet Ecosystem* presso l'Università di Pisa.

rire una omologazione culturale o la costruzione di identità chiuse. Infine, il frequente e generalizzato affidamento *tout court* alle fonti informative presenti online sta ingenerando preoccupanti fenomeni di disinformazione. In questo lavoro, pertanto, si cercherà di analizzare alcuni punti di intersezione tra il pluralismo informativo e i nuovi mezzi di informazione scaturenti dall'era digitale.

2. L'architettura costituzionale e i nuovi media: la convergenza tecnologica

Come è noto, la formulazione testuale dell'art. 21 della nostra Carta Costituzionale esprime, sin dal suo esordio, la volontà di sottolineare un duplice aspetto della libertà di informazione: *in primis*, l'aspetto sostanziale, consistente nella libertà individuale di esprimere il proprio pensiero, ed in secondo luogo l'aspetto strumentale, concernente i diversi mezzi di comunicazione attraverso cui la libertà di espressione può trovare il proprio canale di trasmissione[3]. Si evidenzia perciò un nesso di indispensabile strumentalità tra la disciplina dei mezzi di informazione e gli specifici e diversi contenuti del diritto di libera manifestazione del pensiero, ai fini della piena realizzazione di quest'ultima.

"Libertà di informazione" è quindi un concetto multiforme, più correttamente declinato al plurale che non al singolare: non esiste una sola libertà di informazione, bensì tante libertà quante sono le posizioni che un individuo può assumere rispetto al diritto fondamentale di cui si discute[4]. In questo senso si può distinguere una libertà di informazione "attiva" ed una "passiva". Con la prima accezione si fa riferimento a quella situazione in cui il titolare esercita attivamente il proprio diritto a diffondere e comunicare agli altri consociati le informazioni di cui è a conoscenza, senza alcuna scissione qualitativa ed ontologica tra i diversi contenuti espressivi. In modo complementare, il versante passivo della libertà di manifestazione del pensiero si estrinseca nell'essere destinatario di informazioni. La nostra Costituzione, non curandosi in modo esplicito del profilo passivo della libertà di espressione, ha affidato all'opera degli interpreti l'esplicitazione di uno speculare diritto passivo di essere informati. Tale architettura del dettato costituzionale non deve tuttavia portare alla conclusione che il versante passivo della libertà di espressione sia di minor importanza: la dottrina maggioritaria infatti ritiene che la libertà di ricevere informazioni goda direttamente delle garanzie di cui al 1° comma dell'art. 21 della Costituzione, dal momento che, qualora non si potesse predicare la libertà di ricevere informazioni, verrebbe logicamente ridotto lo spazio del suo predicato logico, ossia la libertà di diffondere informazioni[5].

Dopo questa necessaria premessa definitoria sul contenuto del diritto ad un'informazione pluralistica, occorre evidenziare che la disciplina costituzionale del diritto dell'informazione, incardinata oltre che sull'art. 21, anche sull'art. 15, mantiene una distinzione fra la comunicazione rivolta ad un pubblico indeterminato e quella invece di carattere intersoggettivo. Sebbene un'interpretazione più moderna, che tiene conto dell'impatto delle nuove tecnologie comunicative, tenda a rendere più sfumata tale distinzione, non può non considerarsi il fatto che il dettato costituzionale ponga le basi per una disciplina differenziata dei diversi mezzi di comunicazione, distinguendo fra i mezzi tradizionalmente rivolti al pubblico, quali stampa, radio, televisione, e quelli tradizionalmente destinati alla comunicazione interpersonale e bidirezionale, quali la corrispondenza e la telefonia[6]. Se fino a – relativamente – poco tempo fa, tale impianto rispondeva ad una effettiva divisione strutturale dei mezzi comunicativi ed informativi nel panorama sociale e tecnologico, negli ultimi anni si è assistito ad un fenomeno del tutto nuovo: quello della cosiddetta "convergenza tecnologica". Gli sviluppi tecnologici hanno consentito di diffondere i medesimi contenuti informativi attraverso una pluralità di mezzi diversi e ciascuno di questi mezzi si presta all'erogazione e alla fruizione di servizi legati tanto alla comunicazione informativa di carattere "aperto", quanto a quelle di tipo bidirezionale[7]. La convergenza tecnologica ha di fatto rotto la corrispondenza tra mezzi e servizi, consentendo l'utilizzazione di uno stesso "mezzo" per diffondere una pluralità di "servizi". Non solo. L'avvento di nuove tecnologie informative ha determinato la scissione tra quelli che ormai sono definiti "vecchi media" e "nuovi media", cambiando radicalmente il settore della comunicazione sociale[8] ed arrivando a scardinare irrecuperabilmente il monopolio della diffusione delle informazioni ai media tradizionali.

Risulta quasi scontato rilevare che il ruolo fondamentale giocato in questa transizione tecnologica è stato di Internet, la Rete delle reti. Internet, come noto, è un mezzo capace non solo di immagazzinare dati precostituiti, ma anche di manipolare e costruire informazioni. Partendo dal rilievo che qualsiasi dato inserito può essere letto da chiunque sia in rete in cerca di informazioni, si può dire che più che un mero mezzo di comunicazione, Internet sia piuttosto un servizio informativo diffuso e permanente[9]. Seppur con canali differenti, Internet è uno strumento che costituisce a sua volta un unico ambiente, il c.d. cyberspazio, che rappresenta un reticolo di

contatti, «uno spazio senza collocazione geografica e privo di costruzione gerarchica[10]», dotato di virtù palingenetiche[11].

La sua vocazione alla circolazione di informazioni, alla comunicazione, alla messa in relazione "pariordinata e decentrata", alla costituzione di una comunità virtuale, suggerisce il rilievo materialmente costituzionale del fenomeno Internet[12]. Ed è proprio questa sua attitudine polifunzionale e polimorfa che rende complesso e problematico il rapporto con l'impianto costituzionale moderno, democratico e pluralista. Infatti, se da un lato la Rete viene considerata uno spazio di libertà cosmopolita, in virtù della sua struttura comunicativa, interattiva e pluralista per natura, dall'altro è necessario considerare le implicazioni politico-istituzionali, nonché economiche, di questo spazio di libertà[13].

Per comprendere come l'innovazione tecnologica abbia introdotto un modo radicalmente diverso di produrre e distribuire l'informazione, si possono analizzare due mutamenti significativi. Il primo è, come già evidenziato, l'affermazione di un sistema di produzione dell'informazione totalmente decentralizzato. È infatti sufficiente disporre di un computer o di uno smartphone ed essere connessi ad Internet non solo per poter accedere a qualsiasi tipo di contenuti informativi, ma anche per diventare noi stessi produttori di informazione. Nel nuovo contesto comunicativo, infatti, il singolo individuo assume un ruolo attivo e centrale, cosa che nel "vecchio" assetto era quantomai impensabile, e tale ruolo può estrinsecarsi in una molteplicità di "canali" informativi[14]. La seconda trasformazione, invece, nasce dalla considerazione che per rendere effettivamente utilizzabile da parte degli utenti una tale mole di contenuti informativi, diventa essenziale il ruolo dei soggetti capaci di ordinarla e di facilitare il collegamento tra chi produce informazione e chi vuole riceverla. Si vedrà poco più avanti come alcuni soggetti, in questo nuovo contesto comunicativo, aperto e apparentemente inclusivo, siano detentori in maniera praticamente esclusiva dell'ordine dei contenuti informativi presenti nel cyberspazio: «la rete è aperta ma solo pochi soggetti [...] hanno le chiavi dei cancelli da cui passa l'informazione»[15].

3. Il nuovo assetto dei canali informativi

L'avvento di quella che viene definita, ormai unanimemente, la quarta rivoluzione industriale[16] ha fatto sì che le modalità di manifestazione del pensiero si siano adattate alla nuova "arena" del cyberspazio. Per più di 150 anni, la produzione di informazione e cultura ha avuto necessità di ingenti investimenti per poter raggiungere un numero sempre più elevato di consociati. Gli investimenti in capitali fisici erano indispensabili per organizzare, ad esempio, stabilimenti tipografici, impianti radiofonici, reti telefoniche. Esistevano quindi barriere significative all'ingresso nei mercati dell'informazione, sia per i massicci investimenti richiesti agli operatori, sia per il carattere finito delle risorse su cui si basavano le allora esistenti forme di comunicazione[17]. E se da un lato le Costituzioni riconoscevano a tutti il diritto di manifestare liberamente il proprio pensiero, nei fatti solo quei pochi che avevano accesso a questi limitati e costosi mezzi di informazione potevano effettivamente raggiungere ampie fette di pubblico e concorrere così alla formazione dell'opinione pubblica. Lo sviluppo delle tecnologie digitali, insieme all'avvento di Internet, ha dato inizio a una rivoluzione non solo dei poli di produzione delle informazioni, ma anche degli stessi canali informativi, innescando una crisi dei "vecchi" media che pare irrecuperabile[18]. Pertanto, se da un lato si è potuto assistere alla nascita di contesti informativi del tutto nuovi, quali i social network, dall'altro alcuni mezzi di informazione tradizionali hanno dovuto adattarsi al nuovo spazio digitale. Quest'ultimo è il caso della stampa online.

La stampa online è rappresentata da quelle testate elettroniche realizzate per una diversa modalità di fruizione (la "navigazione in rete") che vengono diffuse con periodicità più frequente di quelle tradizionali[19]. Le testate elettroniche possono esistere in maniera del tutto svincolata ed autonoma rispetto alle omologhe esistenti nel mondo cartaceo o televisivo, oppure possono consistere in una mera replica dei contenuti di quest'ultimi, di cui rappresentano solo una versione più aggiornata e snella. L'analogia dei contenuti ha innescato da subito il paragone tra l'attività di informazione svolta online e la stampa tradizionale[20]. L'assimilazione di queste due attività ha, da un lato, l'effetto positivo di un'estensione allo spazio di Internet di tutte le garanzie tipiche della stampa tradizionale, ma, dall'altro, ha come contropartita la sottoposizione dell'attività online ad una serie di adempimenti e vincoli specifici, *in primis* l'applicabilità ad essa delle fattispecie di reati propri della stampa, quali la diffamazione a mezzo stampa[21] e la stampa clandestina[22]. Nel caso delle testate online iscritte al registro della stampa, la dottrina fa spesso riferimento alla nozione di "stampa telematica", interrogandosi sul regime giuridico ad essa applicabile. Sul punto, l'art. 1 della legge n. 47 del 1948 considera "stampa" tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici in qualunque modo destinati alla pubblicazione. Dopo anni di stagnazione, anche il settore

della stampa è stato sottoposto ad un rinnovamento generale delle regole, allorché il legislatore si è visto costretto a prendere atto dei mutamenti nel frattempo avvenuti nella società scaturiti dall'avanzamento tecnologico. In particolare, la legge n. 62/2001 ha incluso nella definizione di "prodotto editoriale" anche le pubblicazioni su supporti informatici, purché destinate "alla diffusione di informazioni presso il pubblico", con l'applicazione ai medesimi di alcune disposizioni della legge n. 47/1948 sulla stampa. A seguito della modifica operata dalla legge del 26 ottobre 2016, n. 198 all'art. 1 della legge n. 62/2001, il quotidiano online trova per la prima volta una definizione normativa: ai sensi del nuovo comma 3-*bis* dell'art. 1 «per "quotidiano on line" si intende quella testata giornalistica: a) regolarmente registrata presso una cancelleria di tribunale; b) il cui direttore responsabile sia iscritto all'Ordine dei giornalisti, nell'elenco dei pubblicisti ovvero dei professionisti; c) che pubblichi i propri contenuti giornalistici prevalentemente on line; d) che non sia esclusivamente una mera trasposizione telematica di una testata cartacea; e) che produca principalmente informazione; f) che abbia una frequenza di aggiornamento almeno quotidiana; g) che non si configuri esclusivamente come aggregatore di notizie»[23]. Tuttavia, questo esplicito riconoscimento dei quotidiani online da parte del legislatore non consente di estendere ad essi, a tutti gli effetti, gli istituti più caratteristici della stampa cartacea, come il direttore generale o l'obbligo di iscrizione della testata a tutela dei terzi. Il comma 3-*bis* succitato, perciò, ha il solo scopo di fissare i criteri per la percezione dei finanziamenti pubblici e risulta privo di una valenza generale[24].

Gli interventi normativi, tuttavia, non hanno risolto le molte incertezze non solo sul perimetro di concetti quali "prodotto editoriale" e "stampa e stampati", ma soprattutto sull'applicabilità all'attività online della disciplina dei reati a mezzo stampa. Da un punto di vista legislativo, la legge n. 62/2001 non opera un richiamo espresso alle disposizioni penali di cui alla legge n. 47/1948 e ciò sembrerebbe indicare una preclusione dell'applicazione analogica della disciplina dei reati a mezzo stampa ai prodotti dell'attività di informazione online, in ragione del fondamentale principio di tipicità che caratterizza la fattispecie penale. Dall'altra parte, la giurisprudenza, sia di merito che di legittimità, ha adottato negli anni un atteggiamento ondivago[25], fino ad approdare, nel 2015, ad un deciso *revirement* da parte della Suprema Corte, la quale ha abbracciato quelle linee di pensiero più progressiste che caldeggiavano un'assimilazione sostanziale tra la stampa tradizionale e quella telematica, quantomeno per quanto riguarda le guarentigie costituzionali. Con l'importantissima sentenza a Sezioni Unite penali n. 31022 del 2015, infatti, è stato evidenziato che: «Lo scopo informativo è il vero elemento caratterizzante l'attività giornalistica e un giornale può ritenersi tale se ha i requisiti, strutturale e finalistico [...] anche se la tecnica di diffusione al pubblico sia diversa dalla riproduzione tipografica o ottenuta con mezzi meccanici o fisico-chimici»[26]. Alla succitata sentenza della Corte di Cassazione ha fatto seguito una pronuncia delle Sezioni Unite civili che, abbracciando la tesi delle sezioni penali, applica gli stessi principi enunciati con riferimento al sequestro preventivo ex art. 321 c.p.p. al sequestro cautelare di cui all'art. 700 c.p.c., teso ad elidere l'aggravamento del danno patrimoniale e non patrimoniale derivante dalla pubblicazione online di articoli diffamatori[27].

Tali dirompenti sentenze hanno consentito di mettere qualche punto fermo nel panorama della stampa "moderna": pur senza un intervento specifico da parte del legislatore sul punto, può affermarsi che i giornali online, rispettosi dei requisiti organizzativi e di "missione" sanciti dalla Corte di Cassazione, beneficiano delle stesse garanzie costituzionali dei "fratelli" cartacei, in ragione della sostanziale coincidenza delle due modalità informative[28]. Rimane tuttavia aperto un enorme interrogativo: se sia possibile applicare la stessa logica esposta dalla Cassazione anche in riferimento alla normativa penale, data la raggiunta identità ontologica tra la stampa cartacea e quella telematica. L'ostacolo del divieto di analogia in *malam partem* nel diritto penale parrebbe superabile poiché non si tratterebbe di un'interpretazione analogica, bensì di interpretazione evolutiva, la quale porta ad assegnare al termine "stampa" un significato nuovo e più ampio, in linea con i tempi moderni[29].

Dopo la stampa telematica, tra le attività informative online vengono in luce i siti web che, pur non avendo la veste formale della testata giornalistica, contribuiscono a diffondere informazioni in modo sistematico e capillare. È il caso di siti o pagine che pubblicano con modalità atipiche (c.d. post) informazioni che vengono fatte circolare indiscriminatamente tra gli utenti di Internet, tramite collegamento diretto a tali siti o mediante l'accesso agevolato da portali e motori di ricerca specializzati. Esempi tipici di tali mezzi informativi sono i blog, i forum, alcuni social network. Anche in questi casi, come per la stampa online, occorre chiedersi se sia possibile applicare in via analogica o estensiva la disciplina concernente la stampa cartacea, dando prevalenza ad un approccio sostanziale dell'attività informatica[30].

In generale, la giurisprudenza di merito sembrava fare una notevole confusione fra stampa cartacea,

stampa telematica, siti informativi online e semplici manifestazioni del pensiero in rete. Si pensi alle incertezze mostrate inizialmente dai giudici nel distinguere tra facoltà ed obbligo di registrazione dei siti informativi online, da cui rischiava di scaturire una coercizione indiscriminata dei blog e di altre pubblicazioni online a iscriversi ai registri dei Tribunali[31]. Per contrastare tale pericolosa china, è intervenuta la Corte di Cassazione, la quale ha assunto atteggiamenti sempre più restrittivi sul punto, rifiutando in modo risoluto l'estensione analogica ai siti web di informazione della disciplina di matrice penalistica, prima, e delle guarentigie costituzionali riferite alla stampa, poi[32].

Ancora una volta risulta dirimente la sentenza delle Sezioni Unite n. 31022 del 2015, dove si afferma in modo cristallino che, nonostante l'estensione ermeneutica del concetto di "stampa", è necessario tenere ben distinta l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata giornalistica online, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo[33].

Alla luce di quanto detto dalla Corte di Cassazione, dunque, si può affermare che i contenuti informativi rintracciabili su Internet sono soggetti ad una *summa divisio*: da una parte, le testate giornalistiche, dall'altra, tutto il resto[34]. La seconda è una categoria magmatica, composita, in nessun modo sintetizzabile se non da un punto di vista meramente definitorio che, tuttavia, stante il suo carattere evolutivo, non è detto che non possa conoscere, in futuro, una disciplina armonica.

Sul punto è doveroso far menzione ad un preoccupante fenomeno di matrice sociale, legato ai siti informativi online diversi dalle testate giornalistiche, che sempre più sta prendendo piede negli ultimi tempi: quello dell'affidamento generalizzato dell'utenza della Rete ai contenuti informativi presenti online. Infatti, se da un punto di vista normativo ed anche giurisprudenziale non vi è alcuna assimilazione tra i canali informativi tradizionali, quali la stampa e la radiotelevisione, ed i nuovi mezzi d'informazione presenti nella Rete, quali blog, forum e social network, non si può non vedere come una platea sempre più ampia di cittadini dia credito alle notizie circolanti su Internet, indipendentemente dalla fonte consultata.

La Rete, come è noto, rappresenta un significativo spazio di libertà per la manifestazione del pensiero, un luogo dove con un semplice "click" è possibile accedere a milioni di contenuti informativi provenienti da ogni parte del globo. Tale libertà, tuttavia, ha come negativo contraltare una tendenza a considerare i siti informativi presenti nel cyberspazio tutti – o quasi – ugualmente degni di fiducia, alla stregua di un quotidiano o di un telegiornale, che invece, al contrario dei siti presenti nella Rete, sottostanno ad un regime normativo stringente sia per quanto riguarda le loro forme che per certi contenuti. Il discernimento fra ciò che su Internet è effettivamente un contenuto informativo certo e documentato, e ciò che invece appare solo come tale, ma nei fatti non lo è, spesso è rimesso alla sensibilità dell'utente. Tutto ciò comporta un forte cambiamento dell'atteggiamento del cittadino nei confronti della partecipazione informativa alla *res publica*, e ciò pone dei seri interrogativi circa la giustificazione o meno di un intervento più incisivo da parte di una autorità garante[35] ai fini di una consapevole diffusione e ricezione delle informazioni.

4. Nuovi fenomeni informativi nell'era digitale

Fino a qui è stato affrontato il tema delle nuove forme e modulazioni assunte dai canali informativi grazie all'innovazione tecnologica e digitale. È bene ora approfondire un altro significativo mutamento portato dalla nuova era dell'informazione: quello della crescente importanza del ruolo di quei soggetti che "ordinano" e facilitano il collegamento tra chi produce informazione e chi la vuole ricevere[36].

Come è già stato più volte rilevato, la nascita del web ha favorito l'incremento del pluralismo, poiché la Rete ha contribuito all'aumento quantitativo delle fonti consultabili nella valutazione delle notizie, alla neutralità del mezzo rispetto alle informazioni veicolate e all'assenza di controllo da parte dei poteri pubblici o privati – almeno nei paesi democratici – favorita dall'a-territorialità del web. In quest'ottica, il pluralismo dell'informazione ha conosciuto un incremento dato dalla possibilità per le nuove organizzazioni di entrare a far parte del panorama informativo, affiancandosi alle fonti tradizionali e consolidate[37].

La convergenza tecnologica e l'avvento di Internet hanno quindi determinato una circolazione continua ed assolutamente decentralizzata di un'enorme massa di dati informativi. Tale esponenziale diffusione di contenuti ha, ovviamente, molteplici risvolti circa la libertà di informazione – anche – passiva. Infatti, parlando di interesse pubblico all'informazione, non si può prescindere dal considerarlo legato al pluralismo delle fonti, fondamentale per ogni Stato democratico poiché direttamente connesso con il profilo passivo della libertà di informazione stessa, inteso come il diritto a ricevere le notizie da fonti il più possibile diversificate. Per garantire che i cittadini possano esercitare i loro diritti e le loro libertà di scelta e di giudizio, ad essi deve essere garantito

il libero accesso alle informazioni che, come è stato già rilevato, non a caso viene considerato un diritto fondamentale[38]. Il controllo sui flussi di notizie e di dati, al contrario, preluderebbe alla manipolazione dell'opinione pubblica nonché alla concentrazione di potere cui hanno sempre aspirato i regimi autoritari attraverso la censura e il controllo delle reti di informazione. Ancora, da un punto di vista fenomenico, va tenuto in considerazione che una fetta sempre più grande della popolazione recepisce le informazioni "quotidiane" dal cyberspazio, e ciò è agevolato anche dal fatto che i contenuti informativi del web sono spesso gratuiti, e ciò stimola l'interesse e il dibattito pubblico anche di coloro che non acquistano i quotidiani o che non seguono il telegiornale[39].

L'estrema apertura di Internet, però, ha portato a riflettere sulla qualità delle notizie offerte, che molti considerano di scarsa qualità, poiché, logicamente, le fonti non sono sempre verificate o verificabili e costituiscono, in alcuni casi, opinioni del tutto arbitrarie. La multipolarità di Internet è dunque la sua forza, ma allo stesso tempo anche il suo limite, dal momento che ogni utente può pubblicare contenuti senza essere vincolato da norme giornalistiche o di etica professionale, bensì agendo semplicemente sulla base del suo diritto alla libertà di espressione ed informazione[40].

È evidente che, in un contesto del genere, dove non solo i contenuti informativi sono pressoché illimitati, ma anche la possibilità di accedervi è assolutamente libera, coloro che operano una "selezione" dei contenuti attraverso un indirizzamento più o meno invasivo dell'utenza acquistano un potere mastodontico. Tra tali intermediari si annoverano, con ruoli e strutture differenti, i social network ed i motori di ricerca.

Come è facile intuire, questi ultimi hanno un forte impatto sulla mediazione tra contenuti informativi presenti sul web e gli utenti della Rete, poiché essi si pongono come "intermediari digitali" che forniscono l'accesso all'informazione, aiutando il pluralismo inteso tanto come accesso quanto come scelta delle informazioni da parte dei fruitori di Internet. In tal senso, i *search engine* aumentano le fonti da cui attingere e garantiscono la totale personalizzazione dell'esperienza informativa, amplificando il *surplus* informativo tipico della c.d. *information society*. Il loro servizio supporta orizzontalmente coloro che si approcciano al web, aiutandoli a navigare tra le risorse disponibili in rete e orientandoli nel reperimento delle informazioni. Essi, infatti, a differenza di quanto accade con i siti Internet ed i prodotti editoriali, non nascono per soddisfare bisogni specifici, bensì indirizzano l'utente verso il servizio che sta cercando[41]. I motori di ricerca, in un simile contesto, hanno quindi l'importante funzione di mediare tra le fonti di informazione e il pubblico, mettendo a disposizione degli utenti uno strumento essenziale per il reperimento delle notizie che consente di aggregare diverse fonti, siano esse giornalistiche o meno[42].

I motori di ricerca sono dunque le nostre "guide" della navigazione nel web[43]. Essi rappresentano quel necessario meccanismo che seleziona quali informazioni devono raggiungere il lettore – e quali no –. I *search engine* predeterminano l'informazione che viene mostrata all'utente sullo schermo e stabiliscono altresì l'ordine in cui tale informazione viene presentata, determinando in questo modo la sua visibilità[44]. È così che un fatto, un'informazione, una storia può essere indicizzata o no e anche se indicizzata può vedersi assegnato dall'algoritmo un ranking differente da cui dipende la sua effettiva capacità di raggiungere il pubblico. Tutto ciò orienta le scelte dell'utente del web in una direzione oppure in un'altra. E ciò assume ancora più importanza perché, come hanno evidenziato diversi studi di "behavioral economics", la generalità degli utenti ritiene che l'informazione ottenuta dal motore di ricerca sia affidabile, rilevante e neutrale[45].

Si può vedere quindi come il motore di ricerca, rendendo accessibili all'utenza dei significati attraverso delle keyword[46], strutturi uno spazio di secondo livello, dove *significanti* e *significati* si incontrano grazie all'interconnessione tra sistemi di indicizzazione e di ranking[47]. Ed è qui che nasce un problema culturale: come governare il collegamento tra un significato ed un significante? Tale problematica non ha una valenza puramente semantico-stilistica, ma è alla base di qualsiasi politica di Stato: è lo Stato, infatti, il soggetto che si sforza di costruire un linguaggio comune, valevole tra i consociati, ai fini della promozione di interessi comuni. Ed è chiaro come piattaforme quali Google ed altri motori di ricerca, attraverso sistemi di richiami ipertestuali e algoritmi di ranking, stiano di fatto sintetizzando percorsi conoscitivi (pre-)determinati[48]. Detenendo le chiavi dei cancelli da cui passa l'informazione, possono di fatto influenzare l'orientamento degli utenti e quindi la corretta formazione del consenso e perfino la stessa direzione del dibattito pubblico[49].

Come si può comprendere facilmente osservando il funzionamento dei motori di ricerca, il modo in cui viene ordinata l'informazione che appare sul nostro schermo dipende dagli algoritmi impiegati dalle diverse piattaforme[50]. I sistemi impiegati da motori di ricerca e social network sono algoritmi basati su decine di "segnali" elaborati da sistemi di *machine learning*. Ciò vuol dire che il programma ha la capa-

cità di insegnare a sé stesso a partire dall'esperienza ed in questo modo i software imparano dai dati analizzati e "prevedono" il futuro, nel senso che stimano la probabilità di un evento[51].

Anche le notizie vengono distribuite tramite algoritmi e sistemi di *machine learning*. Gli algoritmi "personalizzanti" hanno quindi un ruolo fondamentale nei processi di *story selection*, cioè nella selezione dei contenuti da indirizzare a ciascun consumatore. Sono gli algoritmi a decidere quali notizie e informazioni proporre a ciascun utente, non solo sulla base di meccanismi computazionali a sé stanti ma anche sulla base di specifiche preferenze inferite dai dati ricavati dai precedenti comportamenti dell'utente[52]. Gli algoritmi determinano quali devono essere le notizie e le informazioni che ci raggiungono sullo schermo, ma sappiamo assai poco su come essi funzionano, protetti come sono dalle leggi sulla proprietà intellettuale, e molti utenti neppure pensano al ruolo che essi svolgono quando leggono una notizia, che invece appare loro come oggettivamente rilevante e come frutto di meccanismi tendenzialmente neutrali. Non si può non citare sul punto la calzante espressione utilizzata da Frank Pasquale, illustre professore all'Università del Maryland, il quale, per descrivere la trasformazione che stanno vivendo le nostre società parla di "black box society", sfruttando l'ambiguità semantica di questa espressione[53]. Da una parte, la "scatola nera" registra tutti i nostri movimenti, così come le piattaforme ottengono tutti i dati personali che disseminiamo nel corso della nostra navigazione sul web, per profilarci e poi darci servizi e pubblicità tagliati su misura sulle preferenze di ciascun consumatore. Dall'altra parte, *black box* indica la totale opacità su quello che avviene all'interno della scatola nera e sulla logica seguita per reperire, aggregare, analizzare i dati e predire i comportamenti futuri. In conclusione, quale sarà l'informazione che effettivamente raggiungerà l'utente e influenzerà i suoi comportamenti dipende da un meccanismo avvolto dal segreto e quindi il processo di distribuzione dell'informazione si svolge lasciando chi naviga sul web completamente all'oscuro sulle modalità e i criteri che vengono seguiti[54].

Gli algoritmi usati da motori di ricerca e social media, personalizzanti e dotati della capacità di auto-apprendimento, oltre a selezionare l'informazione da proporre a ciascun utente della Rete, producono un altro effetto molto importante, da tempo all'attenzione degli studiosi: la chiusura dell'utente dentro una "bolla" costruita sui suoi gusti, sulle sue preferenze, sui suoi preconcetti. Nel 2011, Eli Pariser, pioniere dell'attivismo online, colse perfettamente quello che stava avvenendo nel web con il suo libro *The Filter Bubble: What the Internet Is Hiding from You*[55]. In particolare, l'autore già nel 2011 mise in evidenza le conseguenze che sarebbero derivate dalla personalizzazione delle ricerche da *search engine* e social network[56].

La *filter bubble* può essere descritta come quel fenomeno per cui, in un social network che sfrutta degli algoritmi per definire quali siano le notizie di maggior interesse per l'utente, i post visualizzati da un utente sono sempre più in linea con gli interessi ed i gusti dello stesso. L'algoritmo filtra le notizie e le opinioni provenienti dal mondo esterno facendo arrivare sullo schermo solo ciò che è coerente con la visione della realtà di ciascun utente. La conseguenza è che l'utente tende ad essere esposto solamente a quello che è in sintonia con i suoi pregiudizi e, conseguentemente, si rafforza nelle sue convinzioni. L'utente di Internet finisce spesso per ricevere quindi, come notizie e informazioni, soltanto un'eco delle opinioni e dei gusti che ha manifestato (c.d. *echo chamber*) rafforzandosi ancor di più nei suoi convincimenti[57]. Gli algoritmi, di fatto, stanno costruendo un mondo su misura per ciascuno di noi[58]. E se da un lato ricevere informazioni coerenti con le nostre specifiche preferenze è un grande vantaggio soprattutto a livello pratico, le conclusioni cambiano quando si tratta di vedere come la personalizzazione del web condiziona il funzionamento del dibattito pubblico e la formazione del consenso nell'opinione pubblica.

Per comprendere tali conseguenze è utile la distinzione tra la sovranità del consumatore nel libero mercato e la sovranità del cittadino in una nazione libera. Quando si esalta l'informazione personalizzata, facciamo riferimento al consumatore, a cui rendiamo più facili, efficaci e soddisfacenti le sue scelte di consumo. La sovranità politica ha un diverso fondamento perché richiede un dibattito pubblico in cui possano formarsi e confrontarsi idee diverse, uno spazio in cui possano – debbano – trovare accesso anche le idee più lontane dal *mainstream* culturale dominante. In altre parole, nel codice genetico delle democrazie occidentali si trova, fin dalle sue origini, il c.d. *government by discussion*, cioè il principio secondo cui deve essere garantito un confronto pubblico, aperto tra idee diverse e confliggenti, che permetta a ogni cittadino di scegliere la "sua" verità e che non escluda a priori le voci dissenzienti[59].

Al contrario, la *filter bubble* porta alla frammentazione del discorso pubblico ed alla chiusura, piuttosto che all'apertura ed al confronto. Si vengono a creare così comunità chiuse, in cui ciascuno esprime le sue opinioni rivolgendosi esclusivamente a chi la pensa allo stesso modo e riceve notizie e informazioni da chi condivide le sue idee, con la conse-

guenza che l'individuo si rinforza nei propri pregiudizi, ritenendoli l'unica verità, finendo per ignorare o considerare sbagliata, infondata e deviante ogni altra idea o ricostruzione non circolante nella sua comunità virtuale[60].

Come si è potuto osservare, l'avvento di nuovi mezzi comunicativi digitali ha radicalmente cambiato il paradigma del discorso pubblico nelle democrazie occidentali da un duplice punto di vista. Se da un lato ha favorito la diffusione del pensiero alternativo e della c.d. controinformazione, permettendo anche lo sviluppo di innovative e dinamiche forme di democrazia "partecipativa", dall'altro ha incrementato la diffusione di false informazioni con grave nocumento per l'economia e la democrazia. La rete è, nel bene e nel male, «una società c.d. a "potere diffuso" [...] nella gestione della divulgazione di contenuti online»[61] e questo comporta il rischio che la stessa rete sia in grado di inquinare il *public discourse* veicolando informazioni false, le c.d. fake news o bufale[62].

Sebbene tale fenomeno non rientri propriamente nel concetto di "mezzo informativo", ai fini della completezza del discorso qui intrapreso è necessario, tuttavia, accennare a tale distorsione informativa.

Le fake news sono, come suggerisce la terminologia stessa, delle notizie false. Se è pur vero che tali "bufale" non sono estranee al mondo dell'informazione[63], nell'ecosistema di Internet acquistano un'importanza maggiore perché estremamente più ampie sono le possibilità che esse siano prodotte e diffuse capillarmente. Le fake news non hanno nulla a che vedere con le opinioni, in quanto sono vere e proprie menzogne. Sono infatti state definite come quegli articoli recanti notizie che sono intenzionalmente e verificabilmente false che potrebbero trarre in inganno il lettore[64]. Le finalità della diffusione di notizie false possono essere diverse, da questioni personali a motivi economici, o addirittura a esiti politici. In certi casi la circolazione delle fake news avviene con metodi estremamente subdoli: si pensi ad esempio alla creazione di *account* falsi al fine di promuovere esclusivamente fake news, in particolare con lo scopo ultimo di manipolazione politica.

Il problema tecnico che ad oggi si cerca di risolvere è quello della individuazione di meccanismi, criteri e procedure che consentano, magari con l'ausilio degli utenti, di sistemi e di persone che operino un'attività di revisione, asseverando la correttezza o meno di un contenuto informativo[65]. Ciò non appare un fenomeno semplice da gestire, in quanto la circolazione di notizie false ad oggi risulta aggravata dalla mancanza di una regolamentazione di quella particolare "cassa di risonanza" per le notizie che sono i social network, in particolare Facebook. Infatti, se è vero che i social network non producono direttamente notizie e informazione, essi sono ormai uno dei principali strumenti di diffusione di notizie. Il problema principale delle fake news è legato poi proprio all'effetto amplificativo dei social network: senza la portata estensiva e capillare dei social network, con molta probabilità i siti di notizie false non sarebbero così virali[66].

Come è stato osservato, infatti, la allarmante diffusione di fake news sui social network è dovuta sia a meccanismi tecnici e strutturali, sia a motivazioni cognitive/sociologiche. I primi derivano dalla capacità dei social network di raggiungere in maniera unilaterale determinati utenti[67], le seconde sono rappresentate da alcuni fenomeni quali la c.d. *social cascade*, ossia la diffusione a cascata delle informazioni senza un controllo sulla veridicità delle stesse, la c.d. *group polarization*, ossia la polarizzazione "di gruppo", che tende a favorire il rafforzamento di convinzioni all'interno di gruppi omogenei di consociati, ed anche l'influenza delle *prior convictions* (le convinzioni personali) sulla lettura della notizia[68]. A questi caratteri si può aggiungere anche una generale *collective credulity* in relazione ai contenuti online, ossia al fenomeno, in questa sede già commentato, dell'affidamento quasi istintivo dell'utente medio della Rete ai contenuti informativi reperiti online[69].

La diffusione delle fake news non ha trovato ad oggi una risposta efficace da parte del c.d. *marketplace of ideas*[70]. In attesa della formazione di una coscienza critica rispetto ai contenuti diffusi online sembrerebbe indispensabile lo sviluppo di forme di regolamentazione dei social network che siano in grado di prevenire i gravi rischi di inquinamento del *public discourse* legati alla diffusione di fake news sugli stessi[71].

Infine, non si può non accennare ad un altro fenomeno che sta prendendo campo nel settore delle comunicazioni: quello dei c.d. servizi *zero rating*.

Diversamente da quanto analizzato finora in questa sede, tale – potenziale – fattore di polarizzazione delle informazioni diffuse nella Rete non ha un carattere prettamente "sostanzialistico", quale la diffusione delle fake news, ma investe piuttosto la questione della circolazione di notizie da un punto di vista meramente tecnico-tecnologico.

Occorre tuttavia fare preliminarmente delle precisazioni di carattere tecnico. I due principi fondamentali che stanno alla base di Internet prevedono che i messaggi inviati, scomposti in pacchetti di dati in tecnica digitale, siano veicolati attraverso la rete in modo autonomo ("end-to-end") e il più velocemente possibile ("best effort"). In particolare, il principio di trasmissione *end-to-end* sta ad indicare che l'in-

telligenza della Rete, ossia la sua capacità di controllare e indirizzare i dati, è collocata ai piani più alti del sistema "multilivello" di Internet, e dunque nei punti terminali dove l'utente immette l'informazione o utilizza un'applicazione[72], mentre i protocolli di comunicazione, che rappresentano la strada su cui passa l'informazione, devono rimanere i più semplici possibili cosicché nessun terminale possa influire sul percorso seguito dal messaggio nel passare dal mittente al destinatario[73].

Gli effetti positivi prodotti dall'osservanza di questi principi sono molteplici: basti pensare alle innovazioni "in formato digitale" a cui l'ambiente competitivo di Internet ha consentito di approdare grazie alla neutralità della Rete rispetto ai suoi diversi utilizzi, quali il commercio elettronico e la telefonia online. In secondo luogo, la scelta strutturale che i nodi intermedi attraverso cui vengono veicolate le informazioni non possano differenziare i pacchetti di dati in base al loro contenuto o alla loro provenienza ha sostanzialmente assicurato il rispetto di una regola di non discriminazione nell'accesso all'informazione, imponendo di considerare allo stesso modo tutti i pacchetti di dati inviati sulla rete[74]. Ed è qui infatti che emerge il concetto di "Net neutrality": tale concetto rileva innanzitutto come un principio di progettazione, divenuto poi un principio giuridico, e riguarda le reti residenziali a banda larga che consentono l'accesso a Internet, a servizi telefonici e a programmi televisivi. Sebbene non esista una nozione unica e generalmente condivisa, si può considerare neutrale una rete se il traffico (cioè i pacchetti IP) che la attraversa è trattato in modo paritario, senza che gli Internet Service Provider (ISPs) possano operare restrizioni arbitrarie, bloccando o rallentando i dispositivi connessi o facendo pagare diversamente gli utenti finali[75].

Il principio della *Net neutrality* è stato tuttavia messo in crisi dall'aumento esponenziale dei contenuti diffusi in Rete. Ciò ha indotto gli operatori a introdurre forme di intelligenza nella Rete, volte a determinare il contenuto e l'origine dei pacchetti di dati, in modo da disporne un trattamento differenziato[76]. Con l'intento di prevenire o superare la formazione di congestioni di dati, gli operatori che forniscono l'accesso alla rete ISP hanno introdotto in maniera sempre più diffusa pratiche di gestione del traffico consistenti nel reindirizzare, rallentare o velocizzare la trasmissione di alcuni dati rispetto ad altri, segnando così irrimediabilmente il declino dei principi di *end-to-end* e *best effort*[77]. E se è pur vero che tali pratiche di c.d. *network management* si sono rese necessarie, stante l'enorme mole di dati che ogni secondo circolano in rete, dall'altra c'è chi non ha tardato a cogliere in tali differenziazioni del traffico uno spazio di opportunità concorrenziale. In particolare, ciò si è manifestato nell'introduzione di tariffe differenziate per i diversi operatori, penalizzando la trasmissione dei dati di coloro che non siano disposti a pagare per un trattamento preferenziale dei propri contenuti. Appare dunque evidente come la problematica in esame attenga principalmente al diritto della concorrenza dal momento in cui le condotte che pongono limitazioni alla circolazione delle informazioni non si risolvono in semplici riduzioni del traffico dati, ma determinano restrizioni alla libertà di iniziativa economica ed alla concorrenza a danno di operatori presenti attivamente sulla rete[78].

La conseguenza operativa di queste pratiche di gestione è peraltro essenzialmente quella di far viaggiare il traffico dati lungo un doppio binario: uno maggiormente predisposto a congestioni, e quindi di minore affidabilità, e uno capace invece di offrire prestazioni superiori a coloro che siano disposti a pagare di più. Sotto questo profilo il timore che si prospetta, dalla prospettiva dell'utente finale, è che la discriminazione del traffico possa di fatto impedire il raggiungimento di determinati siti web, con il conseguente rischio di compressione del diritto all'informazione[79].

Nel solco di tale prassi concorrenziale, tra le misure di gestione del traffico dati interessate dalle regole sulla *Net Neutrality* sta assumendo un ruolo di rilievo una particolare categoria di pratiche denominate *zero-rating*: esse consistono nell'offerta da parte di fornitori dell'accesso alla rete, prevalentemente mobile, di uno specifico pacchetto di servizi o applicazioni il cui utilizzo è gratuito oppure non viene computato nel consumo del limite di traffico previsto dal contratto per i propri clienti. L'attuazione di queste pratiche commerciali comporta che l'operatore di rete distingua tra diverse fonti di contenuti e servizi, creando per i propri clienti forti incentivi ad accedere ai contenuti e ai servizi loro offerti da alcuni content provider, con i quali hanno stipulato degli accordi, rispetto ad altri. Lampante è quindi il contrasto tra i servizi di *zero-rating* con il principio della *Net Neutrality* secondo cui, come visto, tutti i dati devono essere trattati nello stesso modo[80].

Si deve tuttavia tener presente che questo tipo di iniziative da parte dei principali content provider sono state avviate in mercati particolari, come quelli dei Paesi emergenti (si pensi in particolare a India e Brasile) e più in generale in via di sviluppo (in Sudamerica, Asia e Africa), caratterizzati da un livello di connettività a Internet ridotto e in cui l'accesso alla rete avviene prevalentemente tra dispositivi di telefonia mobile a costi che sarebbero altrimenti proibitivi per la maggior parte degli utenti. L'attuazione di

pratiche di *zero-rating*, in questo contesto, consente di fatto a milioni di persone, che normalmente rimarrebbero escluse, di accedere a Internet. Ciò, tuttavia, ha, tra gli altri, il potenziale effetto dannoso di portare tali utenti ad una percezione errata di cosa sia veramente Internet, inducendoli cioè a identificare i servizi *zero-rated* con l'intera Rete[81].

5. Conclusioni

> *L'enorme moltiplicazione di libri in qualsiasi ambito del sapere è uno dei grandi mali di questo tempo, giacché rappresenta uno dei più seri ostacoli all'acquisizione di una corretta informazione, e getta in faccia al lettore cumuli di cianfrusaglie in cui egli deve cercare a penosi tastoni frammenti di materiale utile*
>
> E.A. Poe[82]

Tale citazione mette provocatoriamente in luce una sorta di "paradosso" informativo: non è detto che più vi sia una moltitudine di fonti informative, e più il cittadino risulti correttamente informato.

Questo perché se da una parte il reperimento e la diffusione delle informazioni sono state rese estremamente più agevoli con l'avvento di Internet, dall'altra l'utente della Rete si trova davanti ad un panorama informativo gerarchicamente confuso e diversamente ordinato, di cui non di rado non si riesce ad individuare la fonte informativa primaria e di cui spesso non si conoscono né si comprendono i meccanismi algoritmici che stanno alla base di ogni ricerca effettuata online. La moltitudine di canali informativi, la singolarità dell'interfaccia attraverso cui tali canali informativi si manifestano, e le forzature commerciali che influenzano la navigazione online sono solo alcuni degli aspetti che stanno potenzialmente determinando un approccio scorretto, o comunque limitato, alla risorsa informativa rappresentata dalla Rete. L'utente, lasciato solo in compagnia di uno schermo, è portato a ritenere che quello che Internet, o meglio, i vari canali informativi che Internet veicola, rappresentino la completezza delle risorse informative. E questo non perché i social network e i blog abbiano il monopolio dell'informazione ma perché, purtroppo, viene incolpevolmente meno la sensibilità della generalità degli utenti di capire cosa ci sia dietro e oltre quello schermo, schermo che viene percepito come un'unica, convergente e neutrale "bocca della verità".

La mancanza di diversificazione dei contenuti informativi trovati in rete ha come sincronica conseguenza la standardizzazione del materiale informativo di cui ogni utente dispone, come suo bagaglio conoscitivo personale. E ciò non perché l'utente ricerchi sistematicamente le stesse cose degli altri *user*, ma perché è l'impianto algoritmico della ricerca online in sé, per come è stato concepito, costruito e poi manipolato, che determina un notevole e sempre crescente livellamento dei risultati delle query[83].

Così l'impianto algoritmico, inteso come l'insieme di regole e meccanismi che intervengono nell'attività di reperimento online delle informazioni, assume metaforicamente le sembianze di Procuste, mitologico brigante, che "livellava" gli sfortunati viandanti fino ad una improbabile *reductio ad unum* di più modi di essere.

Il vero problema legato a fenomeni del genere è un bug nel meccanismo democratico di esercizio consapevole ed informato della sovranità popolare e della partecipazione attiva nello Stato. Ecco perché, innanzitutto, occorre pensare a strumenti idonei a correggere le distorsioni che inevitabilmente si determinano nel nuovo "mercato" dell'informazione. È necessario poi comprendere che in un contesto caratterizzato dall'enorme incremento della capacità trasmissiva, il problema della pluralità delle fonti informative non si pone più tanto in termini oggettivi, come riferito alla pluralità di contenuti presenti nel contesto informativo nel suo complesso, quanto in termini soggettivi, relativamente alla possibilità, per il singolo cittadino, di accedere ad una pluralità di contenuti differenti e scaturenti dai diversi media. È opportuno, infine, riflettere sul ruolo che in questo contesto può svolgere l'esistenza di una categoria di operatori professionali dell'informazione e sulla loro attitudine o meno ad essere adeguatamente formati, riconoscibili e vincolati al rispetto di regole deontologiche comuni[84].

Note

[1] R. Borrello, *Alcune riflessioni preliminari (e provvisorie) sui rapporti tra i motori di ricerca ed il pluralismo informativo*, in "La rivista di diritto dei media", 2017, n. 1, p. 70 ss.

[2] *Ibidem.*

[3] G. Gardini, *Le regole dell'informazione. Dal cartaceo al bit*, Giappichelli, III ed., 2014, p. 50.

[4] *Ivi*, p. 55.

[5] *Ivi*, p. 59.

[6] M.R. Allegri, *Informazione e comunicazione nell'ordinamento giuridico italiano*, Giappichelli, edizione digitale, 2019, p. 229.

[7] *Ivi*, p. 230.

[8] P. Caretti, A. Cardone, *Diritto dell'informazione e della comunicazione nell'era della convergenza: stampa, radiotelevisione, telecomunicazioni, internet, teatro e cinema*, Il Mulino, 2019, p. 195.

[9] *Ivi*, p. 237.

[10] *Ibidem.*

[11]La normativa dell'Unione europea ha definito Internet come «essenziale per l'istruzione e l'esercizio pratico della libertà di espressione e l'accesso all'informazione» (cfr. il Considerando n. 4 della Dir. n. 2009/140/CE).

[12]P. Caretti, A. Cardone, *op. cit.*

[13]Non si può non menzionare il fenomeno dell'*E-democracy*, ossia la democrazia elettronica che procede dal basso (*bottom-up*).

[14]G. Pitruzzella, O. Pollicino, S. Quintarelli, *Parole e potere: libertà d'espressione, hate speech e fake news*, Egea, 2017, p. 57.

[15]*Ivi*, p. 59.

[16]*Ivi*, p. 57.

[17]Quali ad esempio lo spettro limitato delle frequenze disponibili. *Ivi*, p. 55.

[18]*Ivi*, p. 58.

[19]Le testate online vengono infatti aggiornate in modo pressoché continuo nell'arco della giornata.

[20]G. Gardini, *Le regole dell'informazione. L'era della post-verità*, Giappichelli, IV ed., 2017, p. 254.

[21]Cfr. artt. 595 e 596-*bis* c.p.

[22]Cfr. art. 663-*bis* c.p.

[23]Legge 7 marzo 2001, n. 62, *Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n. 416*.

[24]G. Gardini, *Le regole dell'informazione. L'era della post-verità*, cit., p. 256

[25]*Ex multis*, sentt. Cass. pen. sez V, n. 44126/2011, Cass. pen., sez. V, n. 30065/2010, Cass. pen., sez. V, n. 31392/2008, Cass. pen., sez. V, n. 1907/2008.

[26]E ancora sul punto: «L'informazione professionale, pertanto, può essere espressa non solo attraverso lo scritto (giornale cartaceo), ma anche attraverso la parola unita eventualmente all'immagine (telegiornale, giornale radio) o altro mezzo di diffusione, qual è internet (giornale telematico); e tutte queste forme espressive, ove dotate dei requisiti richiesti, non possono essere sottratte alle garanzie e alle responsabilità previste dalla normativa sulla stampa. [...]. Conclusivamente, il giornale telematico, sia se riproduzione di quello cartaceo, sia se unica e autonoma fonte di informazione professionale, soggiace alla normativa sulla stampa, perché ontologicamente e funzionalmente è assimilabile alla pubblicazione cartacea». Sent. Cass. SS.UU. pen. n. 31022 del 2015.

[27]Sent. Cass. SS.UU. civ., n. 23469/2016; G. Gardini, *Le regole dell'informazione. L'era della post-verità*, cit., p. 259.

[28]*Ibidem*.

[29]Ancora sent. Cass. SS.UU. pen. n. 31022 del 2015; *ivi*, p. 260.

[30]*Ivi*, p. 261.

[31]Per esempio sent. Trib. Firenze, I sez. pen., 13 febbraio 2009, n. 983.

[32]G. Gardini, *Le regole dell'informazione. L'era della post-verità*, cit., p. 261 ss.

[33]Sent. Cass. SS.UU. pen. n. 31022 del 2015, in cui, fra l'altro, gli Ermellini analizzano le forme più comuni di siti informativi alternativi alla stampa quali forum, social network, blog.

[34]G. Gardini, *Le regole dell'informazione. L'era della post-verità*, cit., p. 262.

[35]Si è discusso non solo di un possibile autogoverno della rete, ma anche dell'introduzione di Carte dei diritti sovranazionali. Per un approfondimento sul tema, S. Rodotà, *Una costituzione per Internet?*, in "Politica del diritto", 2010, n. 3, pp. 337-352.

[36]G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 58 ss.

[37]L. Bolognini, G. Ragusa, C. Bistolfi et al., *Effetti dei motori di ricerca sul pluralismo dell'informazione. Aspetti giuridici e di analisi econometrica*, 2014, p. 10 ss.

[38]Da un punto di vista di diritto sovranazionale, anche l'articolo 11 della Carta dei Diritti Fondamentali dell'Unione europea afferma che la libertà e il pluralismo dei mezzi di comunicazione devono essere rispettati come elementi essenziali della democrazia promossa dall'Unione, mentre l'articolo 10 della CEDU esclude che «vi possa essere ingerenza da parte delle autorità pubbliche». Cfr. L. Bolognini, G. Ragusa, C. Bistolfi et al., *op. cit.*, p. 10.

[39]*Ibidem*.

[40]*Ivi*, p. 11.

[41]A differenza dell'editoria "nativa digitale", i c.d. "aggregatori", quali i motori di ricerca, i social networks ed altri portali, ai sensi del d.lgs. n. 70/2003 vengono classificati quali "prestatori di servizi nella società dell'informazione" e sono pertanto esenti da una serie di responsabilità in virtù della presunta assenza di controllo del materiale informativo da essi veicolato. R. Borrello, op. cit., p. 11.

[42]*Ivi*, p. 12.

[43]Come "afferma" lo stesso Google, «the Internet... makes information avaiable. Google makes information accessible». G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 62.

[44]In particolare, vi sono tre elementi essenziali del funzionamento del motore di ricerca: il primo è il c.d. *crowding*, ossia la ricerca effettiva dei dati. Vi è infatti un algoritmo (c.d. spider) che "gira" continuamente alla ricerca di informazioni e legge attraverso la semantica i contenuti delle pagine. Il secondo elemento è rappresentato dall'indicizzazione, ossia l'associazione tra una certa ricerca semantica ed un determinato risultato, un "indice" di pagine web. Infine, vi è il c.d. ranking, ossia la gestione effettuata dal motore di ricerca dei risultati delle pagine web emergenti dalla ricerca ed il loro posizionamento nell'elenco indicizzato. Si segnala che tale attività deve essere permessa dai proprietari delle pagine e può essere anche vietata. Google inizialmente poteva andare ovunque nello spazio digitale, oggi invece è possibile precludere l'ingresso al motore di ricerca alla propria pagina web selezionando l'opzione "no spider". Fra l'altro, il *dark web* (ossia uno spazio del web precluso agli spider) ha visto la sua nascita proprio a partire dall'esigenza di non essere "ricercabili".

[45]R. Borrello, op. cit., p. 12.

[46]Le "chiavi di ricerca" a livello semantico.

[47]Da un punto di vista tecnico, l'indagine dei motori di ricerca è così strutturata: il c.d. *crawler* (ossia un software che analizza i contenuti di una rete in un modo metodico e automatizzato) raccoglie le informazioni da un sito di partenza, visitando i suoi *hyperlink* (i collegamenti ipertestuali che rimandano ad altri contenuti informativi presenti nel cyberspazio); i siti che fanno capo agli *hyperlink* sono a loro volta scansionati dal *crawler*, innescando così una ricerca transitivamente progressiva.

[48]Si tratta di capire in che misura un motore di ricerca può promuovere modi alternativi di pensiero. Un esempio che può far capire la silenziosa invasività dei motori di ricerca è il seguente: si ponga il caso di un motore di ricerca che abbia un sistema di blocco per le pubblicità più intrusive, al fine di minimizzare possibili casi di truffe online. Tale blocco potrebbe essere considerato come un principio di censura poiché ad oggi, se un determinato prodotto non ha possibilità di essere pubblicizzato (e pertanto visto) sul web, la diffusione e distribuzione di tale prodotto è destinata al fallimento.

[49]Sul punto non si possono non ricordare i *case study* rappresentati, tra gli altri, dalla campagna elettorale negli USA conclusa con l'elezione di Trump e il referendum in Gran Bretagna per la Brexit. R. Borrello, *op. cit.*

[50] Ai fini del nostro discorso è bene sottolineare che l'algoritmo è un procedimento matematico di calcolo, descrivibile con un numero finito di regole, ovvero un'istruzione proceduralizzata per l'esecuzione di un'operazione più o meno complessa o la risoluzione di un problema.

[51] G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 65. Quando utilizziamo Internet ci imbattiamo frequentemente in sistemi che auto-apprendono: ne sono un esempio i traduttori automatici, i sistemi di raccomandazione di Amazon, Netflix e Pandora, i sistemi di riconoscimento vocale, i filtri anti-spam dei servizi di posta elettronica.

[52] Ad esempio, Google dal 2015 ha introdotto il "RankBrain", un segnale attraverso il quale dovrebbe essere possibile riconoscere il senso della richiesta fatta dall'utente, al di là del fatto che singole parole chiave siano contenute nella sua query. *RankBrain* analizza correlazioni tra più query di ricerca, creando impronte comuni. Pertanto, anche se la ricerca è impostata in modo ambiguo, può comunque ottenere una risposta precisa, proprio perché correlata ad altre ricerche sul medesimo tema. *Ivi*, p. 65.

[53] F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.

[54] G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 65. In realtà, anche le *tech companies* stanno iniziando a rendersi conto che un difetto di trasparenza può pregiudicare la loro reputazione. Così, ad esempio, Google ha iniziato ad adottare delle linee guida che indicano come l'algoritmo dovrà operare. *Ivi*, p. 65 ss.

[55] E. Parisier, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 2011.

[56] G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 67. La personalizzazione delle ricerche è stata introdotta da Google il 4 dicembre 2009. Da quel momento, l'algoritmo di ricerca "Page Rank" iniziò a formulare i risultati più adatti al singolo utente, dando inizio alla c.d. "era della personalizzazione" del web. Un analogo meccanismo di personalizzazione è utilizzato da Facebook.

[57] Il costituzionalista statunitense C.R. Sunstein ha spiegato bene il ruolo delle *echo chambers* nella costruzione del c.d. *daily me*, che si rafforza a seconda del livello di partecipazione, anche politica, nei contesti digitali. C.R. Sunstein, *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, 2017, p. 3 ss., cit. da M. Betzu, G. Demuro, *I* big data *e i rischi per la democrazia rappresentativa*, in "MediaLaws", 2020, n. 1, p. 218.

[58] G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*

[59] *Ivi*, p. 68.

[60] *Ivi*, p. 69. Tale fenomeno prende il nome di "confirmation bias".

[61] E. Falletti, *Internet: la diffusione della cultura non accademica e la formazione dell'opinione pubblica*, in "Cyberspazio e diritto", 2009, n. 3-4, p. 325.

[62] M. Monti, *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, in "Federalismi.it", 2017, n. 24.

[63] Si pensi a quella che è stata chiamata la "Great Moon Hoax": nel 1835 il *New York Times* pubblicò una serie di articoli che parlavano della scoperta della vita sulla Luna. O ancora, alla "Flemish Secession Hoax", quando una stazione televisiva belga pubblicò nel 2006 la notizia che il Parlamento fiammingo avrebbe dichiarato la secessione dal Belgio. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino, S. Quintarelli, "op. cit.", p. 71. Sul punto è opportuno fare un'ulteriore precisazione: sono gli algoritmi stessi, talvolta, ad amplificare la risonanza delle fake news, e ciò per un motivo molto banale: ad oggi, gli algoritmi legati al funzionamento di social network e motori di ricerca, non hanno lo scopo di filtrare le notizie vere da quelle false, ma hanno quello di presentare all'utente notizie in linea con i sui interessi ed opinioni, in modo tale da prolungare il più a lungo possibile la permanenza su una specifica piattaforma digitale. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in "MediaLaws", 2020, n. 1, p. 32.

[64] Definizione fornita da H. Allcott, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, in "Journal of Economic Perspectives", vol. 31, 2017, n. 2, p. 211 ss.; G. Pitruzzella, O. Pollicino, S. Quintarelli, *op. cit.*, p. 73.

[65] S. Quintarelli, Content moderation*: i rimedi tecnici*, in G. Pitruzzella, O. Pollicino, S. Quintarelli, "op. cit.", p. 100.

[66] M. Monti, *op. cit.*, p. 83.

[67] Si tratta del c.d. fenomeno della capillarizzazione dell'informazione.

[68] È istintivamente più facile credere ad una notizia che conferma le proprie opinioni, anziché ad una notizia che le smentisce.

[69] *Ibidem*.

[70] Espressione coniata da John Stuart Mill tesa ad indicare la comunicazione e scambio delle idee intesi secondo il modello dell'economia liberista del libero mercato dove il confronto tra le merci fa prevalere le migliori per prezzi e qualità: allo stesso modo la "libera concorrenza" applicata sul mercato delle idee farebbe emergere le idee migliori, quelle "vere".

[71] M. Monti, *op. cit.*, p. 87 ss. L'inefficacia delle soluzioni giuridiche regolamentari fino ad oggi proposte, quali la rettifica – inefficace per la portata geograficamente più limitata e temporalmente post-datata rispetto alla primaria notizia falsa –, ha portato all'attivazione *motu proprio* di quegli stessi soggetti che sono i "portatori sani" di fake news, quali Facebook. A partire dal 2017, infatti, dopo innumerevoli tentativi fallimentari di lotta alla diffusione di fake news, Facebook ha deciso di intraprendere una nuova strategia di contrasto alle bufale, per il momento solo negli USA. Dopo la segnalazione, attuabile da qualsiasi utente, dei contenuti ritenuti falsi segue un controllo della veridicità della notizia da parte di una squadra di professionisti dell'informazione. Questo controllo è articolato su un *double check* di agenzie di *fact-checking* il cui parere negativo sulla correttezza della notizia comporta la segnalazione della stessa come notizia "non attendibile". Per un approfondimento tecnico sul "content moderation", v. S. Quintarelli, *op. cit.*, p. 99 ss.

[72] Si pensi all'invio di una e-mail.

[73] V. Pampanin, *I nuovi protagonisti del mondo digitale tra neutralità della Rete e accesso all'informazione*, in "Informatica e diritto", 2017, n. 1-2, pp. 237-258.

[74] *Ivi*, p. 238.

[75] R. Calise, *Quattro cose che non sapevi sulla net neutrality: storia di una lite in USA*: «Volendo visualizzare questo concetto, si potrebbe immaginare i *providers* come compagnie postali incaricate della consegna di pacchetti-dati, da porta a porta, passando attraverso il loro centro di smistamento. Questa consegna avviene senza che il *provider* possa regolare la velocità in base al tipo di contenuto del pacchetto dati: non sono possibili riduzioni e aumenti ("throttling") o blocchi ("blocking") della quantità di banda destinata alla trasmissione dei dati, indipendentemente dalla loro natura (o dal loro contenuto)». Fondamentale, sul punto, è stata la sentenza della Corte d'Appello di Washington nel 2014, dove sono state elaborate cinque regole funzionali alla *Net Neutrality*: 1) *No blocking*; 2) *No throttling*; 3) *No paid prioritizazion*; 4) *A catch all standard*; 5) *Transparency*.

[76] V. Pampanin, *op. cit.*, p. 238. Le motivazioni sono state molteplici e vanno dall'esigenza di garantire la sicurez-

za del sistema (si pensi al problema della diffusione di virus tramite spam) al contrasto della criminalità informatica (in riferimento ad esempio alla tutela del diritto d'autore).

[77] *Ibidem*.

[78] *Ivi*, p. 239.

[79] *Ivi*, p. 240. «Il rischio di un abuso dei sistemi di *network management* attraverso il ricorso a pratiche discriminatorie si è effettivamente concretizzato in America, in più occasioni, come nel caso Madison River del 2005, in cui un ISP ha bloccato il servizio di telefonia online di un operatore concorrente; oppure nel caso Comcast del 2007, in cui l'operatore dominante della televisione via cavo in America aveva bloccato applicazioni di *file sharing*». Sul punto: «È tuttavia lo stesso inventore del web Tim Berners-Lee ad aver chiarito che Net Neutrality non equivale a chiedere un'Internet gratis per tutti; assicurare la neutralità della Rete non significa cioè che una persona non debba pagare più soldi per avere un servizio di alta qualità. Viene infatti sottolineato da più parti come la gestione della Rete non possa restare imbrigliata nelle maglie di un controproducente egualitarismo e non debba pertanto seguirsi un'interpretazione assolutizzante del principio di neutralità della Rete, che potrebbe risultare contraria agli stessi interessi degli utenti finali e rivelarsi quindi un ostacolo per lo sviluppo di Internet», *ivi*, p. 242.

[80] *Ivi*, pp. 247-249. In particolare, vengono ricondotte alla categoria *zero-rating* tre distinte forme di *zero-rating*: la prima è quella per cui un content provider si accorda con uno o più operatori di telecomunicazione per fornire ai suoi clienti l'accesso libero e gratuito ad un proprio sito o servizio (*single site/service zero-rating*). La seconda è la pratica cosiddetta degli "sponsored data", in cui un *content provider* paga l'operatore di rete per fornire gratuitamente ai suoi clienti l'accesso a un particolare servizio o contenuto. Infine, l'ultima modalità consiste in una pratica composita, detta "compound zero-rating", grazie a cui una o più società finanziatrici (normalmente grandi *content providers*) si associano a un fornitore di servizi telefonici per garantire ai suoi clienti l'accesso gratuito ad una selezione di siti e servizi.

[81] *Ivi*, p. 250.

[82] Cfr. S. Quintarelli, *op. cit.*, p. 99.

[83] «Perché diavolo Netflix sa sempre esattamente quello che voglio vedere? [...] Forse Netflix ha sviluppato davvero un sistema che è in grado di prevedere i gusti dei suoi utenti e di farlo ragionevolmente bene. Forse questo sistema non è programmato per modificare i nostri gusti [...]. Forse però il sistema sviluppato da Netflix è talmente potente, si è talmente specializzato conquistando sempre più capacità di calcolo, che non si riesce più a controllarlo troppo bene e nessuno sa esattamente in base a quali criteri consiglia quella determinata persona in quel determinato luogo». Cfr. G.L. Conti, *Introduzione*, in M. Pietrangelo, F. Romano, G.L. Conti (a cura di), "Social media e diritti. Diritto e social media", Edizioni Scientifiche Italiane, 2017, p. 31.

[84] M. Cuniberti, *Tecnologie digitali e libertà politiche*, in "Il Diritto dell'informazione e dell'informatica", 2015, n. 2, p. 312.

* * *

Procuste's bed of web informative systems: a fake pluralism?

Abstract: This paper presents an analysis of some of the main issues related to the circulation of information in the Digital Age. The study starts from a general survey of the constitutional architecture and it undertooks a review of the content of the right to inform and to be informed. The study aims to scan the differences between the new and the old *mass media*, focusing on the organization of information channels afterwards the incoming of the Internet, of new information phenomena like fake news and filter bubble, and of the role of intermediaries involved in online research, such as search engines and social networks.

Keywords: Pluralism – Information – Algorithm – Internet

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0033

La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia: quali prospettive future?

Elena Montagnani

Il Web è più un'innovazione sociale che un'innovazione tecnica.
L'ho progettato perché avesse una ricaduta sociale,
perché aiutasse le persone a collaborare, e non come un giocattolo tecnologico.
Il fine ultimo del Web è migliorare la nostra esistenza reticolare nel mondo
Tim Berners-Lee

Prendendo le mosse dall'osservazione dei nuovi paradigmi di comunicazione sociale e dalla loro influenza sulla dialettica dei processi democratici nell'attuale società iperconnessa, l'articolo si propone di indagare le opportunità ed i rischi connessi all'adozione dei nuovi media sociali da parte delle Pubbliche amministrazioni ed il ruolo della comunicazione istituzionale nel processo di trasformazione digitale di queste ultime. Il lavoro intende altresì verificare i limiti dello stato dell'arte e l'adeguatezza degli strumenti tecnici e giuridici messi in campo fino ad ora al fine di avviare una serie di riflessioni sulle prospettive future.

Comunicazione pubblica – Digitalizzazione della P.A. – Infodemia – Cittadinanza digitale – Sovranità digitale – Social media – Cloud – Opinione pubblica – Internet

Sommario: *1. La comunicazione ai tempi della pandemia tra virus materiali ed immateriali – 2. L'influenza della digitalizzazione sulla dialettica del processo democratico – 3. L'amministrazione digitale e i social media: diritti e doveri di essere social – 4. La presenza delle istituzioni sui social media: opportunità o rischio? Quale validità giuridica degli atti della P.A. sui social? – 5. Le varie anime della comunicazione istituzionale ed i social media – 6. La comunicazione pubblica motore del processo innovativo delle P.A.: affacciati sul futuro – 7. È possibile una piattaforma social di pubblica utilità? – 8. La comunicazione istituzionale al centro della trasformazione digitale delle Pubbliche amministrazioni. Conclusioni: verso una riforma della comunicazione pubblica?*

1. La comunicazione ai tempi della pandemia tra virus materiali ed immateriali

La pandemia da SARS-CoV-2 e le connesse situazioni di emergenza e di crisi che ne sono scaturite hanno costituito un punto di osservazione privilegiato dei rapporti tra cittadini, Pubblica amministrazione ed istituzioni, ed hanno mostrato il ruolo centrale della comunicazione pubblica all'interno dell'attuale società iperconnessa. È risultato, infatti, ancora più evidente, a fronte del rafforzarsi di vecchi e nuovi fenomeni quali disinformazione, infodemia, *sharp po-*

E. Montagnani ha conseguito la laurea in scienze giuridiche e la laurea magistrale in giurisprudenza presso l'Università di Pisa con una tesi in sistemi giuridici comparati dal titolo: "La libertà di espressione alla prova delle *fake news*". Ha svolto tirocinio curriculare presso l'IGSG-CNR di Firenze e conseguito il Master in "*Internet ecosystem*: *governance* e diritti" presso l'Università di Pisa.

wer come le istituzioni abbiano un ruolo fondamentale nella gestione della comunicazione e dei flussi informativi verso i cittadini.

A partire da marzo 2020 abbiamo assistito da un lato ad una ricerca spasmodica di informazioni a tema Covid-19 sui principali canali social media, e dall'altro ad un forte incremento delle attività on-line anche in settori tradizionalmente legati ai servizi in presenza (si pensi ad esempio alla scuola, al lavoro, a molti servizi essenziali della Pubblica amministrazione) che hanno dato avvio ad una transizione liquida al digitale.

La pandemia ha costituito per molti versi una spinta verso la digitalizzazione della Pubblica amministrazione, facendo balzare tali temi nei primi posti delle agende politiche italiane ed europee sebbene con un evidente ritardo. Se in passato tale processo aveva fatto fatica ad affermarsi compiutamente a causa sia della scarsa alfabetizzazione e del divario digitale nel nostro paese[1], sia perché non considerato indispensabile da parte dei cittadini che continuavano a prediligere l'utilizzo di servizi in presenza, la crisi pandemica ha reso indispensabile un rapporto di tipo virtuale tra cittadino e Pubblica amministrazione tramite canali digitali.

Nell'epoca della disintermediazione e della sovrainformazione legata anche all'aumento esponenziale dell'uso dei dispositivi mobili, i cittadini, i professionisti, le imprese, ormai da molti anni abitano e sono presenti sui social non solo per relazionarsi con il loro gruppo di pari del settore privato o commerciale, ma anche per ricercare informazioni di ogni genere, comprese quelle relative ai servizi offerti dalla Pubblica amministrazione e di pubblica utilità. Se fino a qualche anno fa gli individui prediligevano quali principali fonti informative televisione e giornali quotidiani, oggi ricercano sempre più nella rete, nei portali on-line e nelle piattaforme social (Twitter, Facebook, Instagram etc.) le notizie di cui hanno bisogno, o meglio vengono raggiunti da una serie di notizie secondo le logiche e le dinamiche proprie dell'algoritmo. Si viene così a creare un patchwork mediale[2] dove il cittadino attinge informazioni da più fonti attraverso una pratica multicanale e crossmediale e che lo vede anche protagonista nella produzione e ridistribuzione con estrema immediatezza e viralità di informazioni, alle quali si assommano opinioni e commenti degli utenti. I social media costituiscono, oggi, qualcosa che va ben al di là di semplici mezzi di veicolazione dei messaggi, sono degli spazi ibridi ed interconnessi, dove circolano e si incontrano non solo idee, notizie e opinioni nei termini più alti della libertà di espressione, ma sono anche uno spazio dove opinioni ed informazioni finiscono per confondersi e dove diventa sempre più difficile per il cittadino distinguere le informazioni "di qualità" da notizie controverse, fake news e da forme di misinformazione e disinformazione più o meno pilotata[3]. I contenuti aventi diversa natura si diffondono in modo capillare in rete e divengono fonti non meramente statiche, ma suscettibili a loro volta di produrre nuove interazioni e nuovi significati da parte dei soggetti che se ne appropriano e li ridistribuiscono e ridiffondono.

Proprio in tale contesto è maturata la convinzione che la tanto annunciata transizione al digitale, quale processo di rinnovamento della Pubblica amministrazione, sia divenuta necessaria e non più procrastinabile, anche a fronte delle misure di distanziamento sociale imposte a salvaguardia della salute dei cittadini. Ed è divenuto ancora più importante creare un sistema virtuoso di comunicazione pubblica, e prospettare un cambio di paradigma nel modo di concepire l'amministrazione, al fine di migliorarne il rapporto con il cittadino.

Questa può costituire, dunque, l'occasione per realizzare quell'idea di *open government* portata avanti soprattutto negli ultimi anni, anche attraverso l'impulso dell'Unione europea, con il Piano Triennale 2019-2021 redatto da AgID, il Piano nazionale innovazione 2020-2025 nonché da ultimo con la Legge 120/2020 (c.d. decreto semplificazioni) e con il Piano nazionale di ripresa e resilienza (PNRR c.d. *Recovery plan*).

Nella contemporanea società dell'informazione, nella quale il principale canale di comunicazione è il social web, i social media possono aiutare a veicolare il messaggio istituzionale in modo estremamente efficace. Possono essere considerati la nuova agorà nella quale le istituzioni incontrano il cittadino? Possono aiutare lo sviluppo di una nuova comunicazione pubblica non più passiva e calata dall'alto ma chiara, "relazionale" e diretta? Essere presente sui social è un diritto dei cittadini o un dovere delle istituzioni? Quali i vantaggi e quali le degenerazioni prospettabili?

Scopo del lavoro è, dunque, quello di verificare i limiti dello stato dell'arte e l'adeguatezza degli strumenti messi in campo fino ad ora al fine di avviare una serie di riflessioni sulle prospettive future.

2. L'influenza della digitalizzazione sulla dialettica del processo democratico

Le nuove tecnologie digitali, l'incremento della capacità di raccogliere, immagazzinare, trattare dati, la connessione permanente che ci consente di essere iper-connessi, la riduzione dei costi di comunicazione hanno innescato una vera e propria quarta

rivoluzione[4] che non riguarda solo i mercati, l'economia o i modelli di business, ma investe e incide profondamente anche sulla produzione e la distribuzione dell'informazione, sulla cultura, sulla politica e sul modo di percepire gli altri e noi stessi. I confini tra vita on-line ed off-line tendono a scomparire, siamo organismi informazionali (*inforg*) connessi gli uni agli altri senza soluzione di continuità: siamo parte integrante di una "infosfera globale"[5]. Si è progressivamente affermata un'idea della rete come espressione dei fenomeni sociali, non legata alla sola dimensione tecnologica ma sempre più inserita nei diversi contesti socio-economici e culturali.

Già il sociologo Manuel Castells, a metà degli anni Novanta, notò come nell'Età dell'informazione i processi dominanti siano sempre più organizzati intorno al concetto di rete[6]. La forma di organizzazione sociale a rete, sebbene non costituisca in assoluto una novità, grazie al nuovo paradigma della tecnologia dell'informazione che ne amplifica la pervasività, va a costituire la nuova morfologia della società, ed influenzare in modo significativo le operazioni ed i risultati dei processi di produzione, esperienza, potere e cultura. In tal senso Castells arrivò a definire la dimensione odierna come una vera e propria network society: una società in rete[7].

Sebbene, quindi, la nascita della network society sia stata in parte favorita da fattori economici, non si può non notare come l'ambito economico sia stato a sua volta influenzato da questo nuovo tipo di struttura sociale. È innegabile come ad oggi l'economia globale sia fortemente orientata a soddisfare i bisogni di una "società in rete", attraverso la produzione, distribuzione e conservazione di informazioni: a dirla con Yochai Benkler siamo di fronte alla *network information economy*[8].

Proprio attratti dalle potenzialità di una tale emergente economia, alcune società private hanno iniziato a fornire servizi volti a razionalizzare e rendere reperibili in modo semplice l'enorme mole di informazioni destrutturate presenti sulla rete Internet.

Oggi questi soggetti, i motori di ricerca e, come vedremo, i social media, con i loro algoritmi stabiliscono la rilevanza delle informazioni e come portieri dell'informazione nel cyberspazio (c.d. *gatekeepers*) detengono le chiavi della rete, accompagnando gli internauti nella navigazione come dei moderni Virgilio danteschi e consentendo ad essi di giungere ai contenuti desiderati o, al contrario, rendendo tali contenuti meno rilevanti.

Nel web sociale i motori di ricerca ed i social media hanno perso il connotato di semplice servizio divenendo un ecosistema di applicazioni ed algoritmi, costantemente disponibili all'utente grazie all'uso degli smartphone e delle "App", il cui scopo è quello di costruire una realtà virtuale liquida e dinamica continuamente alla ricerca di una convergenza con il mondo reale, al fine di mettere in contatto chi produce beni o informazioni con chi ne usufruisce, nel modo più efficace possibile.

Non stupisce quindi che anche a livello statistico emerga come la comunicazione e la distribuzione delle informazioni, oggi, abbia come canale privilegiato proprio quello delle App mobili ed in particolare premi i motori di ricerca ed i social media che per primi hanno sfruttato le potenzialità intrinseche del mezzo per diffondere il proprio modello comunicativo[9].

Per descrivere l'esperienza che stiamo vivendo in un mondo iper-connesso dove non esiste più la distinzione tra essere on-line o essere off-line, prendiamo allora in prestito le parole di Luciano Floridi, il quale ha affermato: «[...] Vorrei descrivere la nostra società come la società delle mangrovie. [...] Le mangrovie crescono in un clima meraviglioso dove il fiume (di acqua dolce) incontra il mare (di acqua salata). Ora immaginate di essere in immersione e qualcuno vi chiede: "l'acqua è salata o dolce?". La risposta è che: "Mio caro, non sai dove siamo. Questa è la Società delle Mangrovie. È sia dolce che salata. È acqua salmastra". Quindi immagina che qualcuno ti chieda oggi: "Sei on-line o off-line?". La risposta è: "Mio caro, non hai idea di dove ti trovi. Siamo in entrambi"»[10]. Siamo, quindi, on-life.

È infatti innegabile che oggi l'individuo percepisca sempre meno la transizione tra mondo reale e mondo digitale, anche grazie al fatto che le reti telematiche si sono evolute verso una struttura molto simile alle reti in cui si organizza la società, caratterizzate da nodi, interconnessioni, legami. Proprio per questo tale costrutto è riuscito a permeare così efficacemente il tessuto sociale, dando vita ad una vera e propria quarta rivoluzione. Ecco allora che ha trovato con il tempo piena concretizzazione l'auspicio del padre di Internet Tim Berners Lee[11], il quale affermava: «Il Web è più un'innovazione sociale che un'innovazione tecnica. L'ho progettato perché avesse una ricaduta sociale, perché aiutasse le persone a collaborare, e non come un giocattolo tecnologico. Il fine ultimo del Web è migliorare la nostra esistenza reticolare nel mondo».

Quello che è possibile rilevare è tuttavia un evidente dualismo che vede da un lato la rete internet (globale, libera, a protocolli aperti e capace di travalicare gli steccati normativi degli stati nazionali), e dall'altro i giganti dell'informazione, i c.d. *Over the Top*[12], i quali, nel tentativo di dare un ordine all'enorme mole di dati destrutturati presenti in rete,

hanno finito per costituire dei punti di accesso all'informazione (privati, a protocolli chiusi e le cui dinamiche sono regolate prevalentemente da algoritmi secondo logiche di mercato).

È quindi chiaro come in una società che fa dell'informazione il proprio prodotto principale, chi controlla l'accesso alla più grande rete di saperi del mondo riveste un ruolo di rilievo all'interno dei rapporti di potere.

Grazie ad una gerarchia liquida, al carattere globale e a-territoriale della rete, al suo travalicare ordinamenti e confini, alla rapidità con la quale le tecnologie mutano e alla volontà iniziale degli Stati di omettere una regolamentazione organica del settore al fine di favorire un nuovo mercato che era apparso sin da subito fiorente, gli OTT si sono mostrati sempre più sfuggenti ad una regolamentazione pubblicistica.

Tutto ciò, unitamente alle dinamiche di funzionamento dei servizi offerti che fanno del dato il "nuovo petrolio", ha consentito alle società pioniere del settore di assumere una posizione di oligopolio se non addirittura di monopolio tanto da aver a poco a poco tracimato la loro dimensione privata e societaria finendo per assurgere a grandi Stati dai confini immateriali, innescando un processo definito da alcuni di "colonizzazione" dello spazio reale[13].

Il ruolo sempre più egemone, assunto dalle grandi piattaforme digitali attraverso i loro servizi, ha delineato nuove dinamiche di interazione sociale e messo in evidenza la difficoltà degli Stati nel padroneggiare i veloci cambiamenti della società legati all'architettura della rete sociale ed alle relazioni sociali che da questa promanano. A tal fenomeno non sono rimaste estranee le amministrazioni degli Stati ai vari livelli, le quali si sono quindi affidate, proprio per la loro efficienza e funzionalità, ai servizi offerti dalle *Big tech*.

Pare opportuno, a questo punto cercare di comprendere il rapporto intercorrente tra Stati e OTT e il ruolo giocato da questi ultimi sia a livello politico che sociale. Ci si è chiesti quindi, se di fronte ad un tale quadro il rischio sia quello di una privatizzazione della sfera pubblica e di una potenziale regressione delle garanzie custodite dalla figura dello Stato costituzionale.

La rete come spazio di libertà, privo di norme, in cui i servizi vengono offerti in maniera "gratuita" dalle grandi piattaforme[14] e le decisioni vengono assunte sulla base del principio di democrazia partecipativa (c.d. *Governance Multi-stakeholder*)[15], conduce al paradigma dell'anarchia intesa come strumento per il superamento dell'istituzione sociale e dell'ordinamento giuridico, per trasformarsi poi in un ordine sociale nuovo: un nuovo ordine spontaneo che come tale è privo di Costituzione, che vede le *Big tech* e le logiche commerciali assumere progressivamente un ruolo preponderante.

Il passaggio dalla legge al contratto, dalle Costituzioni agli standard tecnici e ai *terms of use*, se da un lato risulta un elemento sospinto dalle dinamiche dello spazio globale, dall'altro esula da una visione politica comune e trova il proprio fondamento nella tecnica e nell'economia.

Gli OTT espressione di poteri privati, maggiormente suadenti ed adattivi rispetto ai poteri della sfera pubblica, sono stati considerati maggiormente capaci di governare le logiche non politiche della globalizzazione, non essendo frenati dalle garanzie costituzionali e dai vincoli formali della legge. L'ordinamento globale è stato descritto come un reticolo di regimi parziali, generati da logiche private e guidate da studi legali ed agenzie, sospese in una dimensione liquida tra potere pubblico e potere privato.

Le grandi piattaforme digitali pur essendo molto diverse tra di loro e non avendo tutte la stessa struttura (per fare un esempio Google è altra cosa da Facebook e Amazon non equivale a Twitter) tendono, così come i network finanziari, ad intrecciarsi e muoversi secondo coordinate strategiche simili al fine di ricoprire l'intero spazio di mercato; sembrano non conoscere concorrenza condividendo una visione imperiale di occupazione dell'intero spazio, che li vede incedere compatti, attraverso la continua acquisizione di start-up, integrazioni verticali e progetti condivisi, atteggiandosi, se non addirittura assurgendo, al ruolo di poteri pubblici[16].

Di fronte al quadro appena delineato, allora, i nuovi paradigmi divengono ottimizzazione, efficienza economica, profitto, mentre i diritti fondamentali assumono una dimensione recessiva e minoritaria. Si assiste ad una scissione formale tra sovranità e Stato nazionale, che vede la sovranità riallocata in distinti centri e corpi tecnici corrispondenti alle grandi macro-regioni commerciali, non più corrispondente con lo Stato-nazione.

Il territorio dello Stato-nazione, inteso come delimitazione di un ordine sociale e di un ordinamento giuridico, perde consistenza e si vengono a delineare nuovi confini liquidi costituiti da interessi privati che vanno via via concentrandosi attorno a pochi soggetti che stanno assumendo sempre più sembianze semi-statali.

Le Corporation del digitale sono divenute un semi-Stato, munito di una propria quasi-sovranità, che pur essendo formalmente sottoposto all'autorità degli Stati-nazione, godono di una posizione di privilegio in forza della loro multinazionalità, dei servizi

da esse offerti in modo pressoché esclusivo e della rete sociale quale base creata a livello globale.

Ecco allora che se il codice inizia a penetrare anche nello spazio fisico, inizierà ben presto con il plasmarlo e modellarlo finendo inevitabilmente con incidere sulle libertà e sui diritti costituzionali degli individui: non solo *Code is law* ma *Code is Space* non più virtuale ma sempre più tangibile e reale[17].

Assistiamo a un processo di re-territorializzazione dove il digitale costituisce l'architettura portante di questo nuovo eco-sistema. Si crea una nuova dimensione avente una propria antropologia, proprie istituzioni e una propria dimensione sociale, relazionale, economico-monetaria nonché un potere di risoluzione delle controversie fondato sulle proprie policy (ne è un esempio lampante il nuovo *Oversight Board* di Facebook).

Gli OTT, veri detentori dei codici digitali sono divenuti tasselli distinti ma che si uniscono come un mosaico al fine di esercitare il monopolio informazionale e dei servizi digitali, riuscendo per questa via a conquistare spazi fisici e annichilendo il canone nazionale singolo-sovrano degli Stati-nazione sempre più dipendenti dai dominus della rete.

Come abbiamo accennato, anche gli Stati-nazione sono stati attratti dai servizi che i protagonisti della rete hanno loro proposto, e reso sempre più appetibili e irrinunciabili. Assistiamo a un progressivo processo di appiattimento dei poteri privati sulle funzioni essenziali degli Stati, incarnandone i servizi e facendo leva sulle nutrite comunità virtuali da loro create in rete. Le amministrazioni statali, per intercettare e raggiungere i propri cittadini, hanno spostato proprio in rete gran parte della loro attività di comunicazione e informazione con tutto ciò che ne consegue, come vedremo, in termini di costi e benefici.

Nella società digitale, attraverso il *multi-stakeholderism* i governi, i poteri privati, le ONG, trovano una propria voce nella pluralità di consessi che governano e modellano la rete (si pensi all'ICANN, all'Internet governance forum, all'Internet Engineering Task Force ma anche all'Internet Society ed al World Wide Web Consortium) e costituiscono momento fondamentale di incontro e di scambio sebbene ben lontano dall'idea di Parlamento moderno espressione della volontà popolare.

Ma a ben vedere, nonostante non manchi la partecipazione di una pluralità di soggetti, l'effettivo controllo del web rimane avvinto nelle maglie della Rete ovvero di coloro che hanno facoltà materiale di incidere sulla sua morfologia e sulla espansione virale dei servizi offerti divenuti sempre più irrinunciabili, ovvero nelle mani dei detentori del Codice. A prevalere sono semmai i sistemi di democrazia azionaria interni alle società per azioni[18].

Oggi il web segue essenzialmente regole di mercato e sembra proporsi come spazio aperto, senza padroni, cui tutti possono potenzialmente accedere (*no one owns Internet*), ribelle a qualunque disciplina e refrattario alla regolazione tradizionale. Da più parti si è sottolineata l'esigenza di prendere le distanze da pericolose letture che dipingono Internet come mezzo a-despota, mezzo che sfugge alla possibilità di regolazione degli Stati per la sua dimensione globale. Occorre piuttosto valorizzare la «forza regolatrice dei diritti, che può restituire alla politica il ruolo che le è stato sequestrato dal riduzionismo economico»[19] e sfuggire in questo modo a rischi di oligopolio della rete che vedrebbe quali sovrani le superpotenze o, ancor peggio, i grandi operatori economici del web come Google, Facebook, Apple[20].

È proprio in tale contesto che si inserisce il percorso intrapreso dall'Europa, volto a realizzare una "Europa più adatta al digitale", un mercato unico digitale per l'intera Unione europea. Scopo è quello di tracciare una terza via tecnologica e una nuova governance delle nuove tecnologie rispetto a quella delineata nell'ultimo ventennio da Stati Uniti e Cina.

Oggi il problema principale non è tanto l'assenza di regole (si pensi ad esempio all'ampia regolamentazione in materia di piattaforme a livello comunitario: la direttiva copyright di recente riforma (direttiva 2019/790/UE), la direttiva e-Commerce (direttiva 2000/31/CE), il GDPR (regolamento Ue 2016/679), la *Framework Directive* sulle reti e i servizi di comunicazione(2002/21/CE), la direttiva *Audio Video Media Service* (AVMS) (direttiva 2010/13/Ue), la direttiva per la protezione dei consumatori (direttiva 2011/83/UE), il Codice di condotta sull'*hate speech*[21]), alle quali si affiancano le fonti di *hard law* e *soft law* dei singoli Stati nonché le pronunce dei giudici nazionali ed europei, dando vita così ad quanto articolato connotato da una forte frammentarietà. In tale contesto il rischio è quello di rendere difficile la creazione di un *Digital single Market*. Norme che si presentano spesso come obsolete, poco chiare[22], in una parola inadatte a regolare le nuove realtà, a cui si affianca anche la difficoltà degli Stati nel governare tali servizi, alcuni dei quali hanno via via assunto le dimensioni di "servizio pubblico". Oppure si pensi all'enorme vuoto normativo creato dalla sentenza della Corte di Giustizia europea *Schrems II*[23] che ha invalidato il *Privacy Shield Ue-U.S.* in materia di trasferimento e conservazione dei dati personali extra-Ue. Tutto ciò ha finito per lasciare per decenni la trasformazione digitale nelle mani degli OTT e delle regole di mercato.

Nonostante l'Unione europea il 25 dicembre 2020 abbia presentato importanti proposte in materia di regolamentazione dei servizi digitali (*Digital Service Act* c.d. DSA) e del mercato digitale (*Data Markets Act* c.d. DMA)[24] attese da tempo e volte a regolamentare e riordinare la materia, ancora una volta nel lungo iter normativo hanno avuto un ruolo di primo piano le grandi aziende *tech* accanto a grandi gruppi editoriali e all'industria televisiva e cinematografica, rendendo molto difficile per le associazioni dei diritti civili inserirsi nelle discussioni rilevanti[25]. Uno dei punti salienti della bozza del DSA, riguarda proprio la regolamentazione delle piattaforme e l'uso di sistemi di moderazione e filtraggio.

Tali piattaforme concorrono indubbiamente ad assicurare l'esercizio dei diritti fondamentali quali la libertà di espressione, la libertà di associazione, e costituiscono un importante supporto, tanto più oggi alla prova della pandemia, alla veicolazione delle informazioni ai cittadini, alla educazione e dialogo democratico attraverso anche forme disintermediate di comunicazione tra Pubblica amministrazione e cittadini, anche se nel contempo proprio per la loro struttura congenita consentono anche la diffusione di contenuti illeciti, fake news ed *hate speech*.

La libertà di espressione riveste un ruolo centrale nella formazione e nella sopravvivenza del sistema democratico. Il Parlamento europeo nella risoluzione sulla libertà di espressione del cittadino e la libertà di stampa e di informazione, ha affermato che «la piena esistenza della libertà di espressione caratterizza uno Stato democratico. Il diritto di espressione è un diritto costituzionalmente inalienabile in uno Stato democratico»[26].

Il forte legame che intercorre tra democrazia e libertà da un lato e la capacità di ascoltare, l'apertura alla discussione ed il riconoscimento della legittimità di una opinione diversa dalla propria dall'altro, costituiscono i capisaldi della vita democratica. Affermava Mortati: «Nei sistemi democratici la garanzia di buon funzionamento poggia proprio sulla più ampia libertà di manifestazione del pensiero, essendo essa che alimenta la forza sociale di base, che è la pubblica opinione»[27].

La libertà di espressione e il diritto dell'informazione sono materie vive, in perenne e rapida trasformazione, più di ogni altra branca dell'ordinamento giuridico; sono caratterizzate da un fortissimo legame con le tecnologie di cui si servono per penetrare nella società e raggiungere i loro destinatari. Così come la tecnologia cambia ad una velocità inarrestabile, così cambiano l'informazione e le regole che la disciplinano. E questo è tanto più vero oggi, nella società contemporanea globalizzata, dove una sempre più capillare diffusione di Internet e l'utilizzo dei social media pongono l'individuo al centro di intensi flussi di informazioni che lo vedono allo stesso tempo coinvolto come fruitore e come produttore.

La libertà di espressione ne risulta così ampliata in forma pressoché illimitata ma allo stesso tempo la rete costringe, oggi, ad un ripensamento dei rapporti tra autorità e cittadino e tra potere e opinione pubblica.

È proprio nelle dinamiche relative alla formazione dell'opinione pubblica che trovano legittimazione, in un sistema democratico, le istituzioni e le regole della comunità. Infatti, i processi di legittimazione democratica delle istituzioni traggono il proprio fondamento non solo dall'insieme di regole e procedure formali come le elezioni e il voto parlamentare, ma anche da tutte quelle regole e procedure informali basate sui giudizi in continua evoluzione, quindi sull'opinione pubblica e sugli atteggiamenti di fiducia e sfiducia dei cittadini verso le istituzioni[28].

Vista l'importanza che l'opinione pubblica riveste nel processo democratico andando a delineare i connotati della decisone finale, non solo risulta fondamentale che questa si formi in una agorà dove ascolto, valutazione e critica avvengano in un clima di inclusività e parità delle parti in dibattito, ma è altresì necessario che la qualità del sapere e della competenza su cui tale opinione è fondata sia garantita da contenuti plurali, attendibili ed imparziali[29]. Se è vero che l'opinione pubblica si forma oggi principalmente attraverso i nuovi media on-line, è forse opportuno cercare di capire se questi nuovi mezzi siano in grado di fornire una informazione che sia libera, plurale e quanto più possibile imparziale, presupposti necessari per garantire la formazione di una opinione pubblica di qualità.

Come messo in evidenza da Elis Pariser nel 2011, i social media ed i motori di ricerca non si limitano, ormai, più solo a selezionare l'informazione da proporre a ciascun utente ma chiudono l'utente dentro ad una bolla (c.d. *filter bubble*) costruita su misura sulla base dei suoi gusti, delle sue preferenze, dei suoi pregiudizi. I social network e i motori di ricerca sono, infatti, in grado di sfruttare le informazioni estrapolate dagli algoritmi per definire quali siano le notizie di maggior interesse per l'utente, e proporgli post ed articoli sempre più in linea con i propri interessi e le proprie opinioni. L'algoritmo filtra le opinioni e ci fa arrivare sullo schermo solo ciò che ritiene più vicino al nostro modo di pensare, di vedere ed interpretare la realtà. Gli algoritmi, come dei sarti, cuciono e realizzano sostanzialmente un mondo su misura per noi ed affine ai nostri gusti. Tutto questo, indubbiamente, porta con sé degli enormi vantaggi, riducendo i

tempi e costi di una ricerca, rendendo più semplici e sicuri i nostri acquisti, o aiutandoci a trarre maggiori soddisfazioni nelle interazioni con gli altri.

Sebbene gli algoritmi assolvano pienamente al proprio compito nella sfera economica, tuttavia con il loro progredire è sempre più tangibile l'influenza che essi operano all'esterno di tale sfera, andando ad incidere sui rapporti interpersonali e sociali.

Ecco che l'utente si trova ad essere esposto prevalentemente a ciò che è in sintonia con il suo pensiero, i suoi pregiudizi, i suoi interessi e finisce per ricevere dal web non tanto quello che ha ricercato ma solo una sorta di eco delle opinioni e dei gusti che ha manifestato (quelle che qualcuno ha definito *Echo chamber*)[30]. Il web diviene così un enorme serbatoio di informazioni ma allo stesso tempo un luogo dove l'internauta finisce per rimanere intrappolato in una camera di risonanza, o se preferiamo in una bolla, dove non fa altro che rafforzare i propri convincimenti, in un sistema di autoreferenzialità che altera il modo in cui entra in contatto con il pensiero non affine al suo e non gli consente, per certi versi, di fruire di tutte le informazioni, idee, opinioni che corrono sulla rete[31].

Quando poi tante persone iniziano a vivere nella propria bolla (più o meno consapevolmente) oltre alle conseguenze dirette sul piano personale, iniziano ad innescarsi una serie di conseguenze sul piano sociale: la bolla dei filtri finisce per condizionare non solo la nostra vita ma anche il funzionamento del dibattito pubblico e la formazione dell'opinione pubblica. Questo perché i filtri personalizzati, da un lato ci propongono una sorta di autopropaganda invisibile, ci indottrinano con le nostre stesse idee e dall'altro riducono enormemente, o addirittura fanno venire meno, la possibilità di incontrare idee, esperienze e culture diverse, costruendo intorno a noi un mondo familiare dove però non c'è niente da imparare, dove rimangono vivi i nostri preconcetti, convinzioni e paure. Questo, inevitabilmente, porta con sé una distruzione progressiva del concetto di pluralismo che sta alla base dei sistemi democratici occidentali.

Tuttavia, il cittadino, a differenza del consumatore, ha il diritto e dovere di confrontarsi con argomenti al di fuori della propria sfera di interesse, in modo da poter partecipare a pieno al dibattito pubblico[32].

Allora il problema non è più quello di garantire il pluralismo inteso come efficace sistema di circolazione delle idee, delle opinioni, la presenza del maggior numero possibile di voci nell'area della pubblica discussione, perché questo risultato è stato raggiunto proprio grazie ad Internet. Si tratta piuttosto, alla luce del funzionamento degli algoritmi, dei sistemi personalizzati di selezione delle informazioni, chiusi come siamo nelle nostre bolle e camere di risonanza, di rivedere il concetto di tutela del pluralismo come possibilità di essere raggiunti da una pluralità di opinioni diverse e di informazioni in modo più trasparente e consapevole, di garantire per questa via il confronto, la discussione e la riflessione.

È in questo contesto comunicativo molto complesso che la formazione di una opinione pubblica di qualità, fondata su di una informazione plurale, attendibile ed imparziale, fatica ad affermarsi, andando così a ridurre l'impatto che Internet come rete libera potrebbe avere sul coinvolgimento dei cittadini nel processo democratico.

La distorsione della realtà provocata dalle bolle informative, e la difficoltà di avere una percezione completa e plurale degli eventi, hanno probabilmente contribuito ad innescare polarizzazioni ed un clima di crescente sfiducia e diffidenza nei confronti delle istituzioni e degli esperti del mondo scientifico e giornalistico, i quali sono chiamati ad aggiornare i loro modelli comunicativi rendendoli resilienti alle sfide che i nuovi media pongono.

Gli effetti delle bolle informative hanno recentemente mostrato tutta la loro pericolosità per i sistemi democratici, dimostrandosi in grado di minare alle fondamenta quella che è considerata una delle più grandi democrazie occidentali. In concomitanza della recente transizione dal governo Trump al governo Biden negli Stati Uniti, l'efficacia degli algoritmi di ranking nel rafforzare i pregiudizi e le convinzioni di una parte dell'elettorato ha finito per polarizzare l'opinione pubblica riguardo ad argomenti di importanza cruciale per il processo democratico quali l'esito delle elezioni stesse[33].

Alla luce di tali eventi uno dei più importanti social media, Facebook, ha annunciato che al fine di scoraggiare conversazioni divisive il proprio algoritmo ha smesso di raccomandare gruppi militanti o politici negli Stati Uniti nei periodi precedenti alle elezioni, e che estenderà questa misura anche agli altri paesi nel prossimo futuro. Sebbene Zuckerberg si sia affrettato a precisare che «sarà sempre possibile partecipare a discussioni e gruppi politici per chi lo desidera» è chiaro come ancora una volta una policy arbitrariamente applicata da un soggetto privato vada ad influire in maniera significativa sulle dinamiche democratiche e sulla formazione dell'opinione pubblica.

Vista l'importanza di una corretta comunicazione tra Pubblica amministrazione e cittadini, quale funzione diretta alla realizzazione dell'interesse pubblico, non stupisce l'ampio dibattito che si è venuto a create sulla opportunità per le istituzioni e non solo, di creare nuovi canali comunicativi al fine di sfruttare le potenzialità di questi mezzi e recuperare per questa via un costante dialogo ed un rapporto

diretto e trasparente con i cittadini, fonte di legittimazione per le istituzioni. È tuttavia evidente come questo percorso non sia scevro da ostacoli e debba confrontarsi con le policy ed i sistemi di moderazione di soggetti privati, guidati da logiche di mercato, in cui ogni scelta fatta è orientata a mantenere il massimo livello di appetibilità della propria piattaforma, in contrasto a quello che è l'obbiettivo principale della Pubblica amministrazione ovvero il perseguimento dell'interesse pubblico.

3. L'amministrazione digitale e i social media: diritti e doveri di essere social

A questo punto la domanda che ci dobbiamo porre è: la presenza sui social media è un diritto dei cittadini o un dovere della pubblica amministrazione?

Come abbiamo già avuto modo di vedere, il contesto di riferimento, rispetto al passato, è completamente mutato. Abbiamo assistito negli ultimi anni al dilagare di una serie di strumenti pervasivi quali social media, piattaforme per la condivisione dei contenuti on-line e di collaborazione, blog, che si nutrono di "intelligenza collettiva"[34] e che hanno finito per ridisegnare il modo di esprimersi, relazionarsi, condividere informazioni, informarsi, comunicare.

Ed allora anche la Pubblica amministrazione e le istituzioni non sono rimaste, e non possono rimanere, insensibili a tali mutamenti. Esse sono chiamate a dar vita ad un'opera di reingegnerizzazione dei processi e dei servizi pubblici. In Italia, sotto la spinta del contesto internazionale e soprattutto europeo, sono state intraprese una serie di strategie volte a ridisegnare l'organizzazione delle attività delle pubbliche amministrazioni in chiave digitale. Tutto ciò implica, tuttavia, un profondo ripensamento delle logiche e dei processi dell'*agere* pubblico.

Fine ultimo di tale operazione, intrapresa ormai da anni, non è la digitalizzazione in sé e per sé, né l'aumento dell'efficacia e dell'efficienza delle pubbliche funzioni e dell'erogazione dei servizi attraverso sistemi più celeri e di semplice accesso, ma è quello di garantire, a fianco di una migliore qualità dell'operato della Pubblica amministrazione, una maggiore partecipazione e soddisfazione degli utenti al fine di realizzare un nuovo rapporto di fiducia con essi. Le nuove tecnologie informatiche hanno in sé le potenzialità per garantire una interazione diretta tra cittadino e pubblica amministrazione, per realizzare quei principi di trasparenza, ascolto, partecipazione e collaborazione da sempre auspicati e che affondano le proprie radici proprio nei principi di buon andamento ed imparzialità della pubblica amministrazione (art. 97 Cost.) e nel complesso di norme costituzionali sulle quali si fonda l'ordinamento democratico (artt. 1, 2, 3, 21 Cost.)[35].

Tale processo si inserisce a pieno nel solco tracciato dal modello di *open-government* caratterizzato dai principi di trasparenza (volta a favorire e promuovere l'accountability), di partecipazione (che consente a chiunque di fornire il proprio apporto di conoscenze, idee ed esperienze) e di collaborazione (quale cooperazione tra i diversi livelli di governo e gli attori privati)[36].

Secondo tale modello i governi e le amministrazioni sono chiamati ad essere trasparenti a tutti i livelli e le loro attività aperte all'apporto collaborativo proveniente dalla società civile, al fine di rispondere in modo efficace alle esigenze della collettività. Ci si sposta da un modello fondato sulla logica del procedimento ad un modello fondato sulla logica del servizio, che incentiva l'impiego di strumenti volti a porre al centro il cittadino, al quale deve essere assicurato pieno accesso al patrimonio informativo pubblico. Ciò consentirebbe una partecipazione consapevole ed informata del cittadino e un controllo pubblico sull'operato della pubblica amministrazione[37].

Plasmare il rapporto tra istituzioni, Pubblica amministrazione e cittadino sull'idea di *open government*, passa indubbiamente da un ripensamento delle modalità e degli strumenti attraverso i quali si esplica la relazione con la collettività.

Tra gli strumenti in grado, quindi, di tradurre tali principi in realtà possiamo annoverare, sicuramente, i social media. Strumenti, questi ultimi, in grado di consentire alla Pubblica amministrazione di raggiungere più facilmente e parlare lo stesso linguaggio della comunità alla quale si rivolge, comprenderne le esigenze, interagire con essa con le modalità relazionali più consone e cercare di soddisfarne i bisogni e le aspettative nello svolgimento delle funzioni e nell'erogazione dei servizi[38].

Prima di andare a verificare se esitano nel nostro ordinamento norme che impongano specifici obblighi in capo alla Pubblica amministrazione e alle istituzioni di impiegare i social media quali strumenti di comunicazione e informazione con il cittadino, è opportuno ricordare, come la regolamentazione giuridica del processo di informatizzazione della pubblica amministrazione[39] è risultata operazione complessa a causa, sia della pluralità di fonti che entrano in gioco e dei diversi livelli di governo che sono intervenuti a disciplinare la materia (europeo, nazionale, regionale), sia della stratificazione normativa che si è sviluppata nell'arco di un trentennio.

È opportuno mettere sin da subito in evidenza come tutto ciò sia espressione della difficoltà di regolare una materia in perenne e rapido cambiamento come

quella delle ICT. Il legislatore si è trovato costretto ad inseguire l'evoluzione tecnologica con l'enorme difficoltà di non essere in grado di prevederne gli sviluppi. Ed è in tale contesto che il giurista dovrà cedere il passo ad un approccio connotato da elasticità, flessibilità e mobilità rinunciando per questa via al tradizionale metodo di cristallizzazione di categorie e nozioni fondamentali.

Tutto ciò sembra risponde per un verso al dinamismo fluido del pensiero della c.d. società liquida, dall'altro pone la difficoltà di delineare dei confini chiari, tipici della certezza del diritto, alla quale ogni regolamentazione ed ermeneutica giuridica dovrebbe tendere.

La natura delle fonti in materia di e-government è riconducibile a ben quattro gruppi: gli atti di *soft law* (Agende, Piani, Programmi) [40], le norme di rango legislativo, la disciplina tecnica, gli atti interni emanati dalle singole amministrazioni.

Questa materia per le proprie peculiarità ha dato vita ad un quadro normativo molto complesso caratterizzato da una pluralità di fonti, stratificazioni normative legate sia ai diversi livelli di governo sia alle diverse competenze che entrano in gioco (giuridiche, tecniche, sociologiche).

Tenuto conto poi delle peculiarità tecniche della materia, ai fini della attuazione effettiva delle norme di rango legislativo, si è resa necessaria l'adozione di regole tecniche e di linee guida attraverso atti di natura regolamentare.

A tutto ciò si affiancano una serie di atti interni delle amministrazioni (circolari, regolamenti etc.) con lo scopo di orientare i dipendenti della pubblica amministrazione nella interpretazione di questa stratificazione di fonti nell'esercizio del loro lavoro.

A livello nazionale la l. n. 150/2000 "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni" costituisce tutt'oggi il caposaldo normativo della comunicazione istituzionale. Si tratta dell'unica legge in materia di comunicazione pubblica presente nel nostro ordinamento, la quale ha avuto il merito di aver istituzionalizzato e distinto da altre attività amministrative il campo della comunicazione pubblica, concepita come comunicazione di pubblica utilità e di servizio e non di immagine. Per la prima volta riconosce esplicitamente la necessità che l'istituzione comunichi ed abbia un atteggiamento attivo nei confronti degli amministrati e dei mass media e lo faccia dotandosi di una serie di strutture e professionalità chiamate ad operare in un contesto in cui sono richieste competenze specifiche. In particolare ha tentato di operare una distinzione tra l'attività di informazione (unidirezionale e orientata alla trasparenza) e quella di comunicazione (bidirezionale e orientata ad avviare un dialogo col cittadino e renderlo partecipe nei processi decisionali delle Pubbliche amministrazioni), sancendo il passaggio della comunicazione pubblica concepita come servizio avente carattere meramente strumentale (in particolare si fa riferimento agli istituti che regolano le attività procedimentali della Pubblica amministrazione e all'istituto dell'accesso ai documenti amministrativi l. 241/90) a vera e propria funzione amministrativa[41].

Si tratta di una legge che stenta ancora oggi a trovare compiuta attuazione, ma che intercetta una traiettoria già iniziata con la legge 241/90 sull'accesso ai documenti amministrativi, e con la quale si è avviato un processo di graduale apertura verso il cittadino, passando da un modello autoritativo della Pubblica amministrazione caratterizzato dalla segretezza, a uno partecipativo in cui la trasparenza è la normalità.

Tale percorso è stato poi rafforzato con l'accesso civico semplice (d.lgs. 33/2013) e l'accesso civico generalizzato (Legge delega 124/2015, c.d. Riforma Madia). Si tratta però di processi guidati dalla trasparenza, in un'ottica di informazione e non di comunicazione con i cittadini.

Il processo di apertura verso cittadino è proseguito poi in chiave digitale, ma sempre prevalentemente in ottica di trasparenza, trovando una sua sistematizzazione nel 2005 all'interno del Codice dell'amministrazione digitale (c.d. CAD).

Gli anni duemila hanno visto la diffusione del *multidevice*, la transizione al web 2.0, il diffondersi dei big data e del cloud computing, l'incremento degli ambiti in cui l'adozione di atti amministrativi è stata automatizzata.

Da ultimo, con il d.lgs. 179/2016 l'AgID è divenuta vero motore del processo di digitalizzazione del paese, ed in particolare della Pubblica Amministrazione, essendogli stati assegnati compiti di regolamentazione squisitamente tecnica (fissazione di standard per la digitalizzazione) ma anche un imponente ruolo di programmazione delle fasi di implementazione delle ICT (SPID, CED, FSE, PAgoPA, Cloud, IO.it etc.).

Con il decreto semplificazioni (d.l. 76/2020 convertito l.120/2020) sono stati fissati nuovi obiettivi per la Pubblica amministrazione digitale, sono state previste delle modifiche di ampio respiro a numerosi articoli del CAD al fine di accelerare ed estendere la possibilità per i cittadini di utilizzare i servizi erogati in rete sia dalla Pubblica amministrazione che dai privati. Tale decreto si muove nell'alveo del Piano nazionale dell'innovazione 2020-2025 il quale prevede non solo il potenziamento dell'identità digitale (SPID

e CIE), ma anche l'introduzione di sistemi di notifica a supporto del domicilio digitale (PEC), ed il potenziamento dei servizi fruibili attraverso dispositivi mobili sfruttando l'applicazione IO.

Il processo di digitalizzazione che ha posto sempre più al centro l'amministrato ed i suoi diritti, ha inevitabilmente finito per conferire un ruolo di particolare rilievo alla comunicazione istituzionale, strumento principale per il coinvolgimento del cittadino. Ad oggi non esistono nel nostro ordinamento norme che impongano specifici obblighi in capo alla Pubblica amministrazione e alle istituzioni di impiegare i social media quali strumenti di comunicazione e informazione con il cittadino, tuttavia, un fondamento normativo al loro utilizzo è rinvenibile in più di una norma.

Prima tra tutte la l. 150/2000. In particolare, l'art. 1 c. 4 lett. b) dispone che la comunicazione esterna rivolta ai cittadini, alle collettività e ad altri enti avvenga attraverso ogni modalità tecnica ed organizzativa.

Altresì l'art. 2 c. 2[42] secondo il quale le attività di comunicazione ed informazione della PA «possono essere svolte con ogni mezzo di trasmissione idoneo ad assicurare la trasmissione dei messaggi».

Ad essa si affiancano una serie di altre norme, che seppur non direttamente vanno a toccare in modo tangenziale anche i social media.

Nelle Linee Guida per i siti web della P.A., in particolare all'art. 6 c. 3 relativo alla partecipazione, si afferma che «i social media possono essere considerati dalla pubblica amministrazione come canali di broadcasting ad alto potenziale di audience, dalla forma semplice e di versatile diffusione tra i cittadini, estremamente economici (sia per gli utenti che Amministrazioni pubbliche stesse), multipiattaforma e spesso interoperabili tra loro»[43].

Ancora, la Riforma Madia (l. 124/2015) ha il merito, come abbiamo visto, di aver innescato un radicale mutamento di prospettiva mettendo al centro il tema della cittadinanza digitale con l'obbiettivo di rafforzare e rendere effettivi i diritti digitali dei cittadini nei confronti delle Pubbliche amministrazioni, andando ad incidere profondamente sull'*agere* pubblico e legandolo di conseguenza alla semplificazione dell'accesso ai dati e servizi offerti da quest'ultima.

Alla luce di tale riforma sono stati adottati i d.lgs. n. 179/2016 e n. 217/2017 che hanno operato, come visto, una profonda rivisitazione del Codice dell'amministrazione digitale.

La Circolare n. 2/2017 di "Attuazione delle norme sull'accesso civico generalizzato" nella quale si fa un uso esplicito del termine social media quale strumento utile alla "valorizzazione del dialogo con le comunità di utenti dei social media" (art. 8.2)[44], prevedendo anche che le amministrazioni pubbliche dialoghino con i giornalisti e i media che svolgono attività di *social watchdog* (art. 8.1) che di fatto legittima la pratica di utilizzare il web sociale come fonte giornalistica.

Pur costituendo una libera scelta della Pubblica amministrazione, l'utilizzo dei social media pare incentivato e trovare fondamento normativo anche in tutta una serie di norme del CAD.

L'art. 2 c. 1 nell'individuare le finalità e l'ambito di applicazione del codice dell'amministrazione digitale pare aprire all'utilizzo dei social media nell'ambito dell'informazione e della comunicazione on-line, specificando che «Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione».

Affinché tali obiettivi possano trovare compiuta realizzazione, è però fondamentale che a ciò si accompagni un adeguato livello di alfabetizzazione informatica del cittadino. Proprio sfruttando le peculiarità delle piattaforme social, caratterizzate da un modello di interazione semplice ed intuitivo, non richiedente particolari competenze digitali, che è riuscito ad attrarre in breve tempo utenti aventi estrazione socio-culturale e anagrafica molto eterogenee, le Pubbliche amministrazioni hanno la possibilità di avviare un processo di alfabetizzazione digitale su larga scala, con lo scopo precipuo di ampliare la sfera di utenti dei servizi digitali erogati attraverso le proprie piattaforme, diverse dai social.

Tale processo di alfabetizzazione, pare essere incentivato anche dall'art. 8 il quale prevede la possibilità di avvalersi a tal fine «di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo».

Essendo oggi i social media il principale canale attraverso cui i cittadini si aspettano di ricevere informazioni e comunicazioni anche dalla Pubblica amministrazione, pare pacifico che tra i diversi mezzi menzionati dall'art. 8, questi possano assurgere a ruolo di protagonisti.

L'art. 7, invece, introduce il concetto di qualità del servizio specificando che i servizi on-line erogati dalle Pubbliche amministrazioni devono rispettare «delle disposizioni del presente Codice e degli standard e dei livelli di qualità individuati e periodicamente aggiornati dall'AgID con proprie Linee guida tenuto anche conto dell'evoluzione tecnologica».

Al fine di verificare il grado di qualità del servizio percepito dall'utente al terzo comma tale articolo obbliga le Pubbliche amministrazioni a rendere disponibili agli amministrati sistemi che consentano loro di «di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso all'utente».

Per la loro natura dialogica i social media appaiono strumenti particolarmente adatti a recepire le impressioni degli utilizzatori, le segnalazioni di malfunzionamento o non conformità alle linee guida, permettendo così alle Pubbliche amministrazioni di migliorare la qualità e l'efficienza dei propri servizi. L'utilità dei social media in questo ambito non si esaurisce nel suo utilizzo tradizionale, ovvero nell'interazione diretta tra Pubblica amministrazione ed amministrato, ma apre la strada a nuovi metodi di analisi del grado di soddisfazione degli utenti basati su *machine learning*.

Ne è un esempio significativo la c.d. *sentiment analysis* (nota anche come *opinion mining*), un campo dell'elaborazione del linguaggio naturale che si occupa di costruire sistemi per l'identificazione ed estrazione di opinioni dal testo. Si basa sui principali metodi di linguistica computazionale e di analisi testuale. L'analisi del *sentiment* è utilizzata in molteplici settori: dalla politica ai mercati azionari, dal marketing alla comunicazione, dall'ambito sportivo a quello delle scienze mediche e naturali, dall'analisi dei social media alla valutazione delle preferenze del consumatore[45].

Entrambi questi approcci possono rivelarsi particolarmente efficaci, tuttavia richiedono da un lato l'introduzione di operatori che analizzino i feedback degli utenti provenienti dai vari social e li traducano in una opinione, dall'altro l'introduzione di strumenti tecnologici adeguati che porta con sé la necessità di investimenti in termini economici e di manutenzione.

A fronte delle azioni richieste da parte della Pubblica amministrazione per innescare tale circolo virtuoso, il rischio è quello che si ricorra a strumenti generici (per esempio un classico formulario on-line sulla qualità del servizio) spesso già integrati nelle varie piattaforme informatiche utilizzate per l'erogazione dei servizi on-line (portali, sistemi per la gestione dei contenuti, sistemi per la gestione dei flussi di lavoro, etc...), ma che risultano di scarsa efficacia.

L'art. 7 come abbiamo visto, ha ad oggetto i servizi on-line della Pubblica amministrazione, ma il medesimo approccio sopra descritto può essere riferito anche al coinvolgimento diretto dei cittadini nei processi decisionali e al controllo democratico.

Proprio l'art. 9, dedicato all'*e-democracy*, prevede che le Pubbliche amministrazioni favoriscano «ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili e migliorare la qualità dei propri atti, anche attraverso l'utilizzo, ove previsto e nell'ambito delle risorse disponibili a legislazione vigente, di forme di consultazione preventiva per via telematica sugli schemi di atto da adottare».

La norma prevede che i soggetti pubblici si adoperino al fine di colmare la distanza tra cittadini e decisori attraverso la raccolta di proposte, osservazioni e feedback. Anche in questo caso i social media risultano strumenti particolarmente efficaci nel coinvolgimento dei cittadini nel processo democratico, purché vengano affrontate le tematiche relative al digital divide, e come abbiamo avuto modo di vedere, a tutti gli strumenti necessari alla formazione di una opinione pubblica di qualità all'interno di un complesso contesto comunicativo.

Di non secondaria importanza la portata dell'art. 3 che introduce il diritto all'utilizzo in modo accessibile ed efficace delle soluzioni e degli strumenti adottati dalle Pubbliche amministrazioni anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo.

Tale diritto risulta di contenuto precettivo ed immediatamente applicabile; in caso di violazione, è infatti munito della relativa tutela giurisdizionale davanti al giudice amministrativo così come previsto dal comma 1-*ter*.

È da rilevare quindi che l'art. 3 non riconosce un diritto soggettivo del cittadino e un dovere della pubblica amministrazione nella adozione dei social media, ma nel caso in cui quest'ultima decida, sempre nell'ambito della multicanalità, di impiegarlo attivamente, allora sarà obbligata a garantirne l'accessibilità ed efficacia. Si tratta quindi non di un diritto al mezzo ma di un interesse legittimo al suo corretto funzionamento[46].

Alla luce di quanto sopra esposto, risulta chiaro che pur essendo rintracciabile un fondamento normativo all'utilizzo dei social media da parte delle Pubbliche amministrazione, tale pratica non costituisce un obbligo per la Pubblica amministrazione né un diritto del cittadino al mezzo. Vero diritto del cittadino è invece, quello di ricevere una informazione e una comunicazione pubblica di qualità al quale fa eco un dovere della Pubblica amministrazione di rimettere al centro del suo agire il cittadino e i suoi diritti di essere informato e partecipe della vita civica, anche e non solo attraverso i social media, divenuti ormai l'agorà principale nella quale i cittadini sono presenti ed abitano.

Ad oggi, a fronte del sempre più crescente impiego dello strumento social media da parte delle Pubbliche amministrazioni, un importante punto di riferimento ricco di indicazioni per un corretto utilizzo dei social media in ambito pubblicistico è costituito dal *Vademecum* realizzato da Formez[47] nel 2011, al quale si è affiancato nel 2018 il primo libro *in progress* della nuova comunicazione pubblica in collaborazione con l'associazione PA social dal titolo "Social Media e PA, dalla formazione ai consigli per l'uso"[48].

Sia il *Vademecum* che il nuovo libro, sebbene mettano in evidenza l'assenza di un obbligo normativo della Pubblica amministrazione di essere presente con un proprio presidio istituzionale su uno o più social media, sottolineano l'opportunità di affiancare ai tradizionali canali di comunicazione attraverso i quali vengono erogati servizi e fornite informazioni al cittadino, queste nuove "piazze digitali" dove si trovano la maggior parte dei cittadini e delle imprese al fine di avviare con questi un dialogo. Tutto ciò implica un cambio di paradigma perché non si tratta solo di apprendere le regole di utilizzo di un nuovo strumento di comunicazione ma di avviare un cambiamento culturale profondo sia nelle modalità di erogazione dei servizi sia nel modo di relazionarsi con il cittadino.

Se da un lato tra le parole chiave di questo cambiamento possiamo annoverare comunicazione mobile, app, efficacia, ascolto, dialogo, interazione e partecipazione, fiducia, trasparenza, collaborazione, ottimizzazione dei costi, dall'altro dobbiamo fare i conti con tutti quelli che sono i punti di attenzione delineati, al fine di poterne governare la complessità.

4. La presenza delle istituzioni sui social media: opportunità o rischio? Quale validità giuridica degli atti della P.A. sui social?

Quali sono le opportunità ed i rischi per le pubbliche amministrazioni nella adozione dei social media? Quali sono i vantaggi per la Pubblica amministrazione di essere social? Quali sono le sfide ed i pericoli ai quali si espone?

I cittadini connessi, si aspettano anche dalla Pubblica amministrazione e dalle istituzioni, un modello comunicativo e relazionale analogo a quello che quotidianamente sperimentano nelle pratiche comunicative con il settore privato e commerciale (es. usufruire di servizi on-line o dialogare con i brand in rete). Tutto ciò si lega indissolubilmente al linguaggio[49], ai tempi e alle velocità con cui si muovono i flussi comunicativi sul web, sempre più veloci e liquidi, con i quali la Pubblica amministrazione e le istituzioni sono chiamate a confrontarsi, raccordarsi e sincronizzarsi.

Oggi, in un contesto quale quello della network society, dove la comunicazione assume un ruolo fondamentale, diventa sempre più importante se non addirittura necessario che si realizzi progressivamente un allineamento di tipo culturale tra due mondi ancora troppo distanti tra di loro: quello della Pubblica amministrazione e quello dei cittadini. La Pubblica amministrazione è chiamata a porre al centro la comunicazione e la trasparenza al fine di allontanare progressivamente da sé il peso e la connotazione negativa che ha assunto la parola burocrazia, l'idea di un sistema chiuso e difficile da comprende anche nel linguaggio, lento nei processi e nello svolgimento delle sue funzioni, che negli anni ha finito per allontanarla da coloro al cui servizio essa è preposta, in un clima di progressiva sfiducia.

Nel tempo si è fatta sempre più pressante l'esigenza, per le istituzioni e per la Pubblica amministrazione, di essere presenti on-line con siti web ed in particolare garantendo la loro presenza sui social media, i quali consentono ad esse una interazione maggiore con i cittadini. Diviene allora fondamentale un uso strategico delle ICT, non solo per venire incontro alle esigenze dei cittadini sempre più presenti sui social e per veicolare in modo più efficace i messaggi, ma anche per stabilire con loro un dialogo e dare concretezza alla libertà di espressione intesa come diritto di informarsi, di informare ed essere informati di cui all'art. 21 Cost.

L'assenza della Pubblica amministrazione dalla più grande piazza globale rischierebbe, infatti, di creare un vuoto che difficilmente essa sarebbe in grado di colmare attraverso gli altri media (carta stampata, testate giornalistiche on-line, radiotelevisione, siti web). Partendo dal presupposto che la maggior parte degli amministrati si informa sui social media, il rischio è proprio quello di lasciare il posto a quel flusso di notizie più o meno false, al chiacchiericcio, all'opinione del *quisque de populo* che finiscono altrimenti per prendere il posto dell'informazione di qualità ed acquisirne agli occhi degli amministrati la stessa autorevolezza. Il mondo delle istituzioni ma anche quello del giornalismo, scientifico e accademico, chiusi nelle loro nicchie, con il loro linguaggio spesso difficilmente comprensibile alla maggior parte dei cittadini, con tempi di veicolazione del messaggio lenti, sono stati sempre più messi in ombra dai nuovi comunicatori che spesso si rivolgono alla "pancia" delle masse con un linguaggio familiare, chiaro, semplice, essenziale, veloce, che fa uso anche di immagini, spot e slogan al fine di veicolare in modo più efficace e diretto il messaggio.

A ciò si aggiunge anche un elemento squisitamente tecnico, proprio delle piattaforme social, costituito dall'assenza di un processo di accreditamento degli utenti e di un sistema di identificazione certa dei soggetti che partecipano ad un dibattito. Sebbene alcune piattaforme adottino la politica del "vero nome" per la registrazione degli utenti, questa risulta spesso disattesa e le sanzioni scarsamente efficaci. Tutto ciò, unitamente all'assenza di una chiara segnalazione grafica circa l'autorevolezza o l'autenticità di un profilo, finisce per conferire ad ogni fonte la medesima rilevanza.

Questo nuovo modo di veicolare e di fruire delle notizie ha finito, però, per favorire il diffondersi di fake news, *hate speech*, manipolazione e persuasione dell'opinione pubblica, e abbandonare quel filtro importante di qualità e affidabilità dell'informazione svolto in passato dall'informazione professionale: figure professionali quali giornalisti, addetti stampa, veri e propri *watchdogs of democracy*, aventi capacità di analisi e discernimento delle notizie, sono stati sempre più messi in crisi dai nuovi media[50].

L'assenza delle Pubbliche amministrazioni e delle istituzioni dai social media rischia, quindi, di amplificare tali fenomeni, andando a creare un vuoto non auspicabile proprio su quelle pubbliche piazze on-line dove è di fondamentale importanza la realizzazione di veri e propri "presidii istituzionali" al fine di garantire la presenza di una voce autorevole ed in grado emergere nel rumore di fondo, fatto di notizie e informazioni volte troppo spesso solo a stupire e catturare l'attenzione. Si tratta, quindi, di offrire una informazione certa al cittadino, ed evitare che esso rimanga del tutto intrappolato e fagocitato negli ormai noti meccanismi delle bolle informative e delle camere di risonanza.

Proprio la presenza delle Pubbliche amministrazioni, delle istituzioni e del giornalismo professionale, del mondo accademico e scientifico e anche delle molteplici voci presenti sui social, consentiranno al cittadino di avere a disposizione tutti gli strumenti necessari per costruirsi una propria opinione libera, critica ed informata.

È quindi chiaro che non solo l'assenza delle istituzioni e delle Pubbliche amministrazioni dai social media, ma anche una presenza disomogenea e priva di una strategia comunicativa, rischiano di compromettere i processi democratici e la percezione che il cittadino ha delle istituzioni e rendere la strada che porta alla presenza delle Pubbliche amministrazioni sui social media particolarmente sfidante e non priva di ostacoli e rischi.

L'incedere della Pubblica amministrazione su questo terreno, a partire dal 2009, anno in cui è esploso il fenomeno Facebook, è parso caratterizzato da una certa diffidenza iniziale verso questi nuovi mezzi, e solo alcuni amministratori, cogliendone le potenzialità in termini di visibilità, si sono affacciati sulla piazza del web sociale con un atteggiamento che potremmo definire "spontaneistico" da un lato, e "personalistico" dall'altro. Tale approccio al mezzo era anche favorito da precipue caratteristiche tecniche delle piattaforme social (in particolare Facebook e Twitter), indirizzate inizialmente ai singoli utenti, le quali permettevano esclusivamente l'apertura di profili individuali, poco adatti all'impiego in ambito istituzionale.

In questa prima fase i social media sono stati percepiti da alcuni amministratori più che come nuovo servizio di comunicazione istituzionale a disposizione degli amministrati, come strumenti in grado di fare acquisire loro maggiore visibilità ed ottenere un maggiore consenso, funzionando da vere e proprie casse di risonanza per attività di propaganda.

Fatta eccezione per alcune amministrazioni, le quali sin da subito hanno intuito le potenzialità di questi nuovi mezzi di comunicazione, in grado di espandere in modo strategico e potenziare le attività degli URP, nella maggior parte dei casi essi sono stati utilizzati come vetrine per la pubblicizzazione di eventi, declinandone il paradigma di utilizzo su un modello unidirezionale e divenendo strumenti appannaggio degli uffici stampa.

Ciò ha creato una sorta di *wild west* dei social media, dove a profili più o meno istituzionali si intrecciano quelli personali dei singoli politici, creando una situazione di confusione che rende difficile al cittadino orientarsi in una vera e propria "giungla mediatica" e discernere dove finisce il personaggio politico e dove inizia l'istituzione.

Anche quando Facebook e altre piattaforme hanno consentito la creazione di account istituzionali (ovvero pagine riferite all'organizzazione, *fan/like* page istituzionali, non più solo pagine profilo) utili a favorire una maggiore razionalizzazione della presenza delle Pubbliche amministrazioni sui social media, la maggior parte di queste hanno mostrato una certa difficoltà di coordinamento, creazione e gestione del mezzo (sono infatti numerosi gli account dormienti) e si sono mostrate poco aperte al dialogo e al confronto con imprese e cittadini. Da più parti si è lamentata, infatti, una scarsa capacità di sfruttare la bidirezionalità e le potenzialità di questi mezzi e la mancanza di volontà nell'accogliere in concreto proposte e osservazioni da parte dei cittadini. Nonostante numerose Pubbliche amministrazioni ed istituzioni abbiano cercato negli ultimi anni di porre "ordine al caos" si sono però rivelate poco pronte o

attrezzate a gestire forme non convenzionali di ascolto e relazionalità per venire in contro alle istanze dei cittadini e delle imprese[51].

Occorre, a questo punto, interrogarci anche sulla qualità della presenza istituzionale on-line. Parlare di digitalizzazione della Pubblica amministrazione ed in particolare di "PA social" non significa, infatti, aprire semplicemente una pagina o un canale su piattaforme come Facebook, Youtube, Instagram o Twitter, ma essere disposti ad avviare una trasformazione dei modelli comunicativi e delle forme di partecipazione dei cittadini, delle imprese, delle associazioni secondo un approccio strategico e responsabile, continuativo e *citizen oriented*.

Quanto detto appare ancora più importante alla luce del legittimo affidamento che i cittadini ripongono nei confronti della comunicazione istituzionale effettuata tramite i social media. Molto spesso, infatti, il cittadino è portato a considerare i messaggi provenienti da una fonte istituzionale (che sia una pubblica amministrazione oppure un profilo privato di un soggetto che ricopre una carica istituzionale) attendibili e vincolanti. Tuttavia, come ha avuto modo di precisare la Corte di Cassazione civile nella sentenza n. 70/2002 la volontà di obbligarsi di una Pubblica amministrazione non può desumersi implicitamente da fatti o atti, ma deve essere manifestata nelle forme tassativamente indicate dalla legge[52].

Pertanto, un tweet o un post su Facebook, sebbene proveniente da un soggetto istituzionale (si pensi ad un Sindaco o ad un Ministro), non ha validità giuridica e vincolante sebbene sia capace di orientare le scelte dei cittadini. Come sottolineato infatti dal Consiglio di Stato con sentenza n. 769/2015[53] avente ad oggetto la comunicazione di un Ministro attraverso i social media e la sua natura di atto amministrativo, il ricorso a forme di comunicazione non tradizionale, per quanto in principio ammissibile, non genera in capo all'amministrazione gli stessi vincoli che nascono con l'esercizio di attività amministrativa ordinaria, né ovviamente produce gli stessi effetti nella sfera giuridica dei destinatari[54].

È chiaro, quindi, come una comunicazione informale sui social media di bassa qualità, spesso di puro stampo propagandistico, rischi di ingenerare nell'amministrato false aspettative e di conseguenza di allontanare il cittadino dalla vita pubblica incrinandone il rapporto con la Pubblica amministrazione e le istituzioni[55].

Pare allora evidente come risulti necessario individuare una strategia comunicativa alla luce della quale avviare una serie di attività fondamentali, quali: selezionare i contenuti da inserire nel piano editoriale, stabilire una social media policy sia interna che esterna (volta a delineare regole di condotta degli utenti sulla piattaforma e un patto di reciproco ascolto e dialogo tra Pubblica amministrazione e cittadini), individuare figure professionali *ad hoc*[56] costantemente aggiornate in grado di realizzare un solido e sinergico sistema di comunicazione maggiormente in sincronia con la società, in grado di guidare le amministrazioni nella sfida che la digitalizzazione pone superando la retorica dell'innovazione[57].

Altrettanto importante è lo sviluppo di una architettura digitale di ascolto delle esigenze dei cittadini[58] volta a misurare l'impatto delle attività e delle scelte della Pubblica amministrazione sul tessuto sociale. Questo può avvenire sia attraverso una comunicazione diretta (si pensi all'URP sempre più chiamata ad operare su un piano di multicanalità) che attraverso l'utilizzo di strumenti di *social media mining* e poi di *sentiment analysis*. Tutto ciò richiede tuttavia un forte investimento in termini di risorse e di tecnologia che rende questa attività di appannaggio quasi esclusivo delle grandi amministrazioni, limitando di fatto le potenzialità che l'impiego delle piattaforme social potrebbe avere nel riavvicinare gli amministrati ai loro amministratori.

Proprio per descrivere la situazione relativa alla eterogeneità del tessuto amministrativo (ad es. amministrazioni centrali e periferiche, sanità, università etc.) è sorto in letteratura il concetto di *assembled mix*[59], un processo di assemblaggio di componenti tecniche, giuridiche ed istituzionali frutto di interventi umani, culturali e tecnologici, che pur nel rispetto di principi generali deve essere calato sulle caratteristiche precipue di ogni singola realtà amministrativa. Proprio la necessità di diversificare l'approccio alla comunicazione pubblica sui social media in base alle specificità dei vari enti, può rendere necessario anche un ripensamento dei modelli organizzativi interni e richiedere l'introduzione di nuove strutture o uffici. Tuttavia, la tendenza della macchina organizzativa pubblica è da sempre quella di resistere al cambiamento prediligendo la reiterazione di prassi di lavoro e principi organizzativi ancora legati al modello burocratico weberiano[60], rendendo problematica, anche data l'assenza di un obbligo normativo, l'introduzione delle piattaforme social nel modello comunicativo dell'amministrazione.

Oggi la tendenza è quella di cercare di individuare all'interno della pubblica amministrazione una struttura dedicata alla comunicazione sui nuovi media, dotata degli strumenti e delle professionalità necessarie (si pensi al dibattito sull'attribuzione di tali funzioni all'URP oppure all'Ufficio stampa o ancora alla creazione di nuove strutture dedicate), caricandola di una discrezionalità nella scelta dei contenuti

da pubblicare, nei tempi e nei modi di pubblicazione, nella scelta dei canali; scelte che spesso sono guidate da logiche propagandistiche, piuttosto che da vere e proprie esigenze comunicative.

Tuttavia, la trasversalità di un ambito comunicativo che permea tutti i processi amministrativi pare suggerire, invece, un approccio meno centralizzato e che necessita di una strategia a più ampio spettro che coinvolga tutte le strutture ed i processi operativi.

Questo modello affonda le proprie radici nella predisposizione di un piano strategico di comunicazione pubblica caratterizzante ciascun ente, il quale si concretizza in un processo che fissa le fasi in cui si articola la creazione e la pubblicazione di un messaggio, le regole di interazione tra i vari uffici, le responsabilità di ciascuno di essi, e le modalità di raccolta e analisi dei feedback.

In tale processo ogni ufficio o struttura che svolge una funzione o offre un servizio che necessiti di essere veicolato verso l'esterno, sarà chiamato ad elaborare il contenuto del messaggio ed individuarne le finalità; sarà poi un soggetto o una struttura di raccordo che, in possesso degli strumenti e delle professionalità necessarie in ambito non solo tecnologico ma anche giuridico, comunicativo ed organizzativo, si occuperà di tradurre quel messaggio nella forma e nel linguaggio più consoni allo specifico canale e al pubblico al quale si rivolge, anche tenendo conto delle finalità indicate. La stessa struttura di raccordo sarà chiamata altresì a raccogliere mediante l'interazione umana o gli strumenti già citati di *sentiment analysis*, i feedback e le richieste degli amministrati, veicolandole nel linguaggio e nella forma più appropriate all'ufficio interessato.

Tutto ciò consente in primo luogo, grazie all'introduzione di regole ben precise riguardanti le responsabilità e l'interazione tra i vari soggetti, di eliminare gli elementi di discrezionalità prima citati, ed in secondo luogo di migliorare l'efficienza e l'efficacia della comunicazione pubblica garantendo sia una maggiore trasparenza dell'operato della Pubblica amministrazione, sia la possibilità, grazie all'interazione continua con i cittadini e le imprese, di migliorare i servizi offerti.

Ecco che la comunicazione pubblica assume così una rilevanza tale da assurgere non a mero servizio pubblico (inteso come attività meramente materiale, strumentale, o momento finale di un procedimento amministrativo espressione di una funzione pubblica) ma a vera e propria funzione amministrativa autonoma, intesa come attività giuridica caratterizzata da proprie strutture, procedure e figure professionali, in grado se non di garantire, quantomeno di favorire la trasparenza tanto auspicata dell'operato della Pubblica amministrazione[61]. Una Pubblica amministrazione sempre più dialogante ed aperta al cittadino nello svolgimento delle proprie funzioni e nella assunzione delle proprie decisioni, dove l'amministrato diviene sempre più partecipe e co-decisore.

Non dobbiamo, infatti, trascurare un'altra questione che si pone al di sopra di tutte quelle trattate fino ad ora: la redazione della social media policy deve essere coerente con i termini di servizio (c.d. TOS) dei social media. Essendo questi ultimi soggetti a frequenti aggiornamenti la Pubblica amministrazione dovrà monitorarne l'evoluzione al fine di valutare se le modifiche intervenute siano in linea con la missione dell'ente. Tuttavia, è bene evidenziare che le piattaforme social sono gestite da soggetti privati e che i termini di servizio riflettono esigenze di marketing e sono orientati a mantenere alta l'appetibilità della piattaforma per gli utenti. Non necessariamente le modifiche apportate a questi termini di servizio sono guidate da principi compatibili con quelli dell'ente o dell'istituzione, primi fra tutti la pubblica utilità e il buon funzionamento della Pubblica amministrazione, nonché la libertà di espressone intesa in senso ampio come libertà di esprimere la propria opinione, informarsi e informare da parte del cittadino. Può quindi accadere che a seguito di una modifica delle TOS di una piattaforma social, si debbano rivedere le proprie social media policy interne ed esterne e, dove questo non fosse possibile per incompatibilità nella missione perseguita, valutare l'abbandono della piattaforma.

Proprio quest'ultimo aspetto sottolinea l'importanza di un approccio comunicativo orientato alla multicanalità al fine di garantire l'incontro tra le Pubbliche amministrazioni e il cittadino indipendentemente dalla disponibilità di una particolare piattaforma. Se da un lato come abbiamo visto l'abbandono di un social media può avvenire per decisione della Pubblica amministrazione, dall'altro può essere la piattaforma stessa ad interrompere l'erogazione del servizio attraverso sistemi di moderazione dei contenuti o addirittura la cancellazione o la sospensione di un profilo.

Ne sono testimonianza anche i recenti avvenimenti che hanno visto coinvolte alcune piattaforme social ed il Presidente uscente degli Stati Uniti Donald Trump, alla vigilia della cerimonia di insediamento del presidente neoeletto Joe Biden. A seguito di un mandato presidenziale caratterizzato da aspri contrati tra il Presidente Trump e le piattaforme social (in particolare Twitter), in cui queste ultime hanno marcato alcuni suoi post come "argomento controverso", abbiamo assistito dopo gli avvenimenti del 6 gennaio 2021 di Capitol Hill, alla sospensione del pro-

filo del Presidente. Questa estrema misura, sebbene da molti celebrata ed a lungo auspicata, altro non è che l'espressione di continue violazioni contrattuali da parte dell'utente Trump ed ha avuto un impatto talmente significativo sulle quotazioni di mercato del titolo Twitter[62] da spingere quest'ultimo a revocare la sospensione solo 12 ore dopo averla attuata salvo poi ripristinarla in via definitiva[63].

Sebbene quindi i social media possano essere uno strumento in grado di migliorare la comunicazione ed i rapporti tra Pubblica amministrazione e cittadino, la loro natura privatistica e le logiche squisitamente economiche che li guidano, li rendono altamente volubili ed inaffidabili e pongono le istituzioni e la Pubblica amministrazione nella condizione di approcciarsi a questo mezzo con una giustificata cautela, nonostante esso rappresentati la piazza digitale più frequentata dai cittadini.

5. Le varie anime della comunicazione istituzionale ed i social media

La comunicazione pubblica si articola in comunicazione istituzionale, politica e sociale[64]. Alcuni autori hanno messo in luce la parziale sovrapponibilità tra questi tre ambiti comunicativi ed hanno individuato una classificazione ancora più dettagliata della comunicazione proveniente dalle istituzioni pubbliche ed in particolare amministrative[65].

Occorre a questo punto chiederci se i social media, sicuramente in grado di assicurare pubblicità e maggiore trasparenza delle scelte e dell'operato delle Pubbliche amministrazioni, siano adatti a veicolare i messaggi di tutte o solo alcune tipologie di comunicazione istituzionale, tenuto conto non solo delle peculiarità del mezzo ma anche dei tipi di dato trattato[66].

Volendo muovere dall'articolazione della comunicazione istituzionale proposta da Franca Faccioli, questa è caratterizzata da cinque dimensioni: la comunicazione normativa, la comunicazione delle attività istituzionali, la comunicazione di pubblica utilità, la comunicazione per la promozione d'immagine, la comunicazione sociale[67].

Alla base della comunicazione istituzionale pubblica si pone la comunicazione normativa che costituisce momento fondamentale per una corretta formazione dell'opinione pubblica ma anche e soprattutto strumento attraverso il quale far conoscere a tutti i cittadini le regole del vivere sociale, i loro diritti ed i loro doveri.

Come abbiamo già avuto modo di vedere, la conoscenza delle leggi, dei decreti, dei regolamenti e di ogni altra fonte normativa nazionale e sovranazionale è presupposto di ogni relazione consapevole tra cittadini e tra questi e gli enti pubblici. A fianco dei siti web istituzionali, i social media possono costituire un valido alleato per veicolare i testi normativi ai cittadini in modo facile, veloce e capillare e metterli a disposizione, gratuitamente, al *quisque de populo*[68]. Questo tipo di comunicazione, proprio per il messaggio che è chiamata a veicolare presenta i caratteri della universalità e genericità, non tratta dati personali per i quali è necessaria una particolare attenzione, e non richiede l'identificazione del destinatario del messaggio. Può altresì costituire una importante cartina di tornasole per monitorare il punto di vista dei cittadini sulle norme adottate, attraverso commenti e le opinioni[69]. È fondamentale però che sia ben riconoscibile al destinatario il soggetto che le mette a disposizione.

La comunicazione delle attività istituzionali è, invece, l'azione comunicativa volta ad illustrare le attività delle istituzioni dello Stato ed in particolare delle amministrazioni e del governo. Questo tipo di comunicazione è quella che più di ogni altra rischia di scivolare verso la propaganda e quindi verso una comunicazione di tipo politico. Non è sempre facile, infatti, distinguere la natura degli atti di promozione istituzionale dagli atti di promozione politica, entrambi voluti da chi ricopre i vertici di una amministrazione pubblica (si pensi ad esempio ad un Ministro, ad un Sindaco, ad un Presidente di Regione). Questi soggetti si trovano contemporaneamente nella posizione di esponente della maggioranza di governo e di capo dell'amministrazione, ma mentre i primi si rivolgono ai cittadini elettori, i secondi si rivolgono ai cittadini amministrati[70].

Difficilmente il cittadino sarà in grado di comprendere a quale titolo venga veicolato un determinato messaggio e se lo scopo sia quello di informare sui risultati raggiunti dall'istituzione o sia strumento di mera promozione del personaggio politico.

Gli slogan ed il linguaggio utilizzato, talvolta aggressivo, rissoso, di basso livello[71], spesso figlio di un pensiero strategico ben preciso e pianificato che fa leva su rabbia, tristezza e paure dei cittadini, uniti alle peculiarità del mezzo (in particolare la disintermediazione, la "targettizzazione" degli utenti, la diffusione capillare, le ricondivisioni, la possibilità di applicare la *sentiment analysis*[72] per analizzare le reazioni degli utenti anche attraverso lo studio di emoticon e commenti etc.) e alla decontestualizzazione finiscono per disorientare il cittadino.

Il rischio è quindi quello di equiparare gli account social dei singoli politici che ricoprono cariche istituzionali alle istituzioni stesse o al contrario

sfruttare gli account istituzionali per trasmettere un messaggio strettamente politico.

Nonostante la l. 150/2000 abbia cercato di delineare una più chiara distinzione tra attività di comunicazione e informazione al fine di creare una demarcazione tra il messaggio politico e quello istituzionale, né questa né l'applicazione delle norme sul silenzio elettorale da parte sia delle istituzioni che dei partiti (l. 212/1956 più volte modificata; l. 81/1993; l. 515/1993 e l. 28/2000) sembrano essere in grado di arginare tale fenomeno[73].

A tale proposito potrebbe essere di aiuto la predisposizione di una serie di regole chiare sui soggetti-uffici chiamati ad utilizzare tali media (URP, Ufficio stampa, Social media manager etc.), ma anche la previsione di un obbligo di comunicazione delle attività istituzionali attraverso un linguaggio di tipo impersonale, in modo da rendere più chiaro e riconoscibile al cittadino chi sta' diffondendo il messaggio, quali siano le finalità sottese ed offrire contenuti informativi neutrali. Pare quindi opportuno un intervento da parte del legislatore al fine di regolamentare non tanto il mezzo ma la condotta dell'istituzione sul mezzo nella sua attività di comunicazione di attività istituzionali.

La comunicazione di pubblica utilità si caratterizza, invece, per la sua dimensione di servizio, e ha quale scopo principale quello di informare i cittadini sulle modalità di funzionamento degli uffici e sulle prestazioni offerte. In questo caso i social media, ma anche l'uso di app, possono costituire un valido alleato per la Pubblica amministrazione per potenziare l'impianto di informazione e comunicazione tradizionale (incontro diretto con il cittadino c.d. servizio di front-office, o per via telefonica) oppure quello più recente che sfrutta la rete informatico-telematica (e-mail; siti Internet), utilizzati per diffondere informazioni ma anche come mezzi di ascolto e dialogo con il cittadino e l'impresa, andando così ad estendere soprattutto l'attività degli URP o degli uffici preposti a diffondere ad ogni livello informazioni agli utenti.

Il social media proprio perché disintermediato e di facile fruizione da parte dell'utente, ha in sé le potenzialità per creare una relazione diretta con il cittadino, un luogo di accesso informativo e di rivendicazione del servizio. Gli URP finisco per questa via, per diventare simbolo di una burocrazia flessibile, dialogante e disposta all'ascolto. Inoltre, la Pubblica amministrazione e le istituzioni, attraverso l'accoglimento dei feedback degli utenti raccolti per mezzo dei social media, possono venire più facilmente a conoscenza di quelli che sono i bisogni e le opinioni sui servizi offerti ai cittadini (c.d. *customer satisfaction*), svolgere indagini sulla *web reputation* dell'ente e sulla base di questi migliorare i servizi ed il sistema organizzativo.

Questo è tanto più vero se pensiamo alla comunicazione per la promozione d'immagine. I social media, in grado di raggiungere il cittadino non solo attraverso testi scritti o audio ma anche e soprattutto attraverso la potenza delle immagini, posso rivelarsi molto utili per promuovere e migliorare l'immagine delle istituzioni e degli enti, attraverso la realizzazione di politiche di costruzione dell'immagine secondo i canoni del marketing, simili a quelle utilizzate per le imprese del mercato privato.

Tuttavia, non dobbiamo dimenticare il fine ultimo di tale attività: quello di migliorare la credibilità, l'affidabilità e la fiducia che i cittadini ripongono nei confronti della propria amministrazione e delle istituzioni.

Per non correre il rischio che tali operazioni siano controproducenti e finiscano per disaffezionare il cittadino, è quindi necessaria una certa coerenza tra ciò che una campagna di promozione di immagine di un ente dice di esso, e ciò che lo stesso ente fa.

A fianco della comunicazione istituzionale troviamo la comunicazione sociale. Con il tempo la comunicazione sociale è divenuta anche una componente della comunicazione dell'istituzione pubblica. Per molti anni è stata, infatti, di esclusivo appannaggio di enti non- profit o imprese private, le quali avviando campagne di sensibilizzazione e di orientamento dei comportamenti sociali su determinati temi di interesse collettivo (si pensi a temi quali l'ambiente e la sostenibilità, la salute e la prevenzione, l'emarginazione sociale, la sicurezza sul lavoro, l'ordine pubblico e la sicurezza sociale, la violenza e la parità di genere, il bullismo, le crisi umanitarie, l'abbandono e il maltrattamento di animali etc.), hanno svolto un ruolo di vera e propria supplenza dello Stato[74].

Da prima la televisione e a seguito il web si sono dimostrati particolarmente efficaci nel veicolare il messaggio portato da tali campagne di comunicazione sociale. I social media (in particolare YouTube, Instagram, Facebook particolarmente adatti ad ospitare video ed immagini che più di ogni altra cosa sono in grado di impressionare l'utente), grazie ai meccanismi di ricondivisione, in grado di autoalimentare la campagna e permeare in modo virale, capillare, veloce tutta la rete sociale sembra essere il mezzo che più di ogni altro è adatto a raggiungere lo scopo. Altresì, come per altri tipi di comunicazione il suo carattere bidirezionale può fungere da termometro delle opinioni dei cittadini su determinati problemi di interesse collettivo.

Non si esclude che le piattaforme social possano costituire anche un valido strumento di "cittadinan-

za attiva" ovvero un luogo dove gruppi di cittadini particolarmente sensibili a determinate tematiche si confrontano tra di loro e dove possano incontrare gli Uffici preposti di Istituzioni e Pubbliche amministrazioni e dialogare con loro proprio per realizzare in modo sinergico campagne di comunicazione sociale su temi di interesse pubblico comune, al fine di sensibilizzare anche altri soggetti, tenuto conto però delle considerazioni appena svolte.

Per ultima, ma non per questo meno importante, la comunicazione interna della Pubblica amministrazione. Per anni, la comunicazione tra uffici e tra Pubbliche amministrazioni, è stata concepita come gerarchica, formale, e caratterizzata da iter burocratici rigidamente scanditi da circolari ed informazioni di servizio calate dall'alto anziché organizzata sulla capillare diffusione e condivisione di informazioni e conoscenze a tutti i livelli. Solo con la l. n. 150/2000 si è iniziato a riconoscere l'importanza di una comunicazione interna basata su di un maggior dialogo e partecipazione del personale appartenente ai vari uffici, settori, servizi, coinvolti nelle varie fasi dei processi decisionali, strumento propulsore per stimolare una riorganizzazione del lavoro in chiave più flessibile e funzionale al fine di offrire un servizio più efficiente che porti con se anche un miglioramento della comunicazione esterna e del rapporto con il cittadino.

Una buona comunicazione interna favorisce una maggiore cooperazione e interazione tra gli uffici ed ha un ruolo strategico nella diffusione di valori e conoscenze al fine di migliorare la produttività e la risoluzione dei problemi[75].

Negli ultimi anni la diffusione dell'uso dei social media nella comunicazione interna, a fianco di strumenti cartacei, circolari informative, intranet, e-mail, riunioni operative, manuali di comportamento organizzativo, bacheche (tradizionali ed elettroniche), è stata rimessa alla spontanea adozione di alcune Pubbliche amministrazioni che ne stanno sperimentando l'impiego a supporto di attività di coordinamento di gruppi, per velocizzare lo scambio di informazioni e la assunzione di decisioni durante il lavoro quotidiano soprattutto nelle Amministrazioni più complesse e articolate o tra il personale di Amministrazioni diverse, dove lo scambio di informazioni tra professionisti e gli incontri "faccia a faccia" in un determinato giorno, ad una determinata ora e in un determinato luogo possono non essere agevoli ed immediati.

I social media ed i sistemi di messaggistica come Whatsapp, le piattaforme di videoconferenza come Zoom, Skype, Hangouts, etc. possono favorire indubbiamente il lavoro cooperativo a distanza. Tuttavia, se il loro impiego consente di superare una serie di ostacoli e barriere, favorire una maggiore trasparenza nei processi decisionali interni, e modalità più flessibili di approccio al lavoro agevolando la cooperazione, allo stesso tempo impone una serie di attenzioni soprattutto per quanto concerne la normativa sulla privacy. Affinché tali strumenti siano utilizzati in modo ottimale è opportuno che i vertici di ciascuna amministrazione approntino chiare regole di utilizzo che i dipendenti saranno chiamati a seguire (c.d. policy interna).

L'organizzazione di questo tipo di comunicazione, come emerge dai tavoli di lavoro promossi a livello nazione dalla rete URP degli URP[76] nei suoi 15 anni di attività e oggi dal Dipartimento della funzione pubblica, è affidata in alcune realtà ad un ufficio *ad hoc* che si affianca all'URP, all'Ufficio stampa e al Portavoce, mentre nelle realtà più piccole è interamente curata dal personale URP. Tuttavia, l'incedere del processo di digitalizzazione della Pubblica amministrazione ha mostrato come una figura *ad hoc*, in grado di coordinare e pianificare tutta l'attività di comunicazione interna ed esterna, sia sempre più indispensabile.

In generale è proprio il progressivo processo di digitalizzazione della Pubblica amministrazione a richiedere un ripensamento delle vecchie logiche burocratiche e l'introduzione di nuove modalità di organizzazione dei processi di comunicazione sia interna che esterna, nonché di produzione, condivisione, scambio delle informazioni.

Nella comunicazione interna, quindi, l'adozione di social media risulta compatibile in particolar modo, seguendo la definizione di Invernizzi, con la comunicazione strategica, creativa e formativa, le quali hanno ad oggetto la condivisione di procedure, metodologie e materiale di carattere pubblico e generale. Al contrario una comunicazione di tipo funzionale, la quale spesso ha ad oggetto procedimenti ed atti caratterizzati dalla presenza di dati personali, risulta particolarmente refrattaria all'utilizzo delle piattaforme social.

Le Pubbliche amministrazioni devono, quindi, muoversi nell'alveo tracciato dal GDPR quando si trovino a pubblicare e trattare dati personali (in particolare artt. 4, 5, 6, 9, 17 GDPR) e questo risulta particolarmente rilevante quando la comunicazione avvenga attraverso piattaforme di soggetti privati aventi sede in Stati al di fuori del territorio dell'Unione Europea, le quali spesso non offrono le medesime garanzie (artt. 44-50 GDPR)[77]. Inoltre, il passaggio attraverso una piattaforma terza, integra le caratteristiche di diffusione di dati personali che l'art. 2-*ter* del d.lgs. 101/2018 definisce come «il dare conoscenza dei dati personali a soggetti indeterminati, in qua-

lunque forma, anche mediante la loro messa a disposizione o consultazione» e dovrebbe essere ammessa da parte delle P.A. unicamente quando è prevista da una specifica norma di legge (conformemente all'art. 6, par. 1, lett. c, GDPR).

Questo avviene in quanto il canale rappresentato dalla piattaforma social non si configura come un mezzo di trasmissione neutro ma come un vero e proprio soggetto terzo, che accede all'informazione e la utilizza dichiaratamente per i propri fini (es. analisi di mercato) e ciò a differenza di quanto avviene ad esempio nell'utilizzo di una pec la quale garantisce che solo il destinatario possa accedere al contenuto del messaggio escludendo i gestori del servizio.

Pertanto, prima di pubblicare e diffondere on-line informazioni (sia attraverso l'uso di social media, sia con siti istituzionali) attraverso atti, documenti amministrativi e allegati contenenti dati personali (sia nel processo di comunicazione interna che esterna), le P.A. dovrebbero effettuare una valutazione rigorosa rispetto alla materia della protezione dei dati e verificare che la normativa in materia di pubblicità preveda tale obbligo, al fine di evitare di perdere il controllo sui dati personali pubblicati.

La Pubblica amministrazione sarà quindi chiamata a rispettare tali principi, non solo quando si tratti di pubblicare informazioni con finalità di trasparenza così come richiesto dal d.lgs. 33/2013 ma anche in tutti gli altri casi di pubblicità (integrativa dell'efficacia, dichiarativa, notizia) necessari a garantire la pubblicità legale degli atti amministrativi o volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza. A titolo esemplificativo, si pensi alle pubblicazioni di deliberazioni, ordinanze e determinazioni sull'albo pretorio on-line degli enti; matrimonio; atti concernenti il cambiamento del nome; comunicazione di avviso deposito delle cartelle esattoriali a persone irreperibili etc.

Alla problematica legata al trattamento dei dati personali nell'uso dei social media, si affianca quella relativa alla impossibilità di identificare in modo certo tutti gli interlocutori. Infatti, le principali piattaforme social non consentono una identificazione forte (c.d. *strong authentication*) dell'utente, rendendo di fatto impossibile stabilire se il destinatario sia veramente chi sostiene di essere, sia esso un cittadino, una impresa o una Pubblica amministrazione. Proprio per questo viene meno la certezza che l'interlocutore sia effettivamente legittimato ad entrare in contatto con il dato personale anche in presenza di un profilo certificato (si pensi al bollino di certificazione di Facebook) in quanto le credenziali utilizzate per l'accesso a tale profilo non rispettano i criteri di sicurezza richiesti per una identificazione certa come avviene invece per altri protocolli come Spid o CIE.

Pare dunque pacifica l'inadeguatezza dello strumento del social media quale canale di comunicazione nelle casistiche che coinvolgano una comunicazione funzionale agli atti sia essa interna o esterna, riducendo l'uso di questo particolare strumento ad un mero sistema di notifica, scevro da qualsivoglia dato personale, andando così a diminuirne sensibilmente l'effettiva efficacia ed utilità rispetto ad altri mezzi.

Questi che si presentano come ostacoli all'utilizzo delle piattaforme social in alcune delle attività della Pubblica amministrazione, possono fornire spunti interessanti per spingere la digitalizzazione della P.A. verso una "socializzazione" dei propri processi, sfruttando le caratteristiche che hanno determinato il successo di questi nuovi media, ma tenendo sempre ben a mente quei valori e quei principi che, come abbiamo visto, animano e che debbono animare l'operare della Pubblica amministrazione.

Questo consentirebbe anche di operare la tanto auspicata riprogettazione dei processi amministrativi, ormai obsoleti, in chiave digitale, abbandonando la pratica fin troppo comune di un appiattimento delle nuove tecnologie sui vecchi processi.

6. La comunicazione pubblica motore del processo innovativo delle P.A.: affacciati sul futuro

La pandemia ci ha insegnato che la comunicazione costituisce elemento essenziale della formazione dell'opinione pubblica, fondamentale per il coinvolgimento di istituzioni, imprese e cittadini in quella che sarà la ripresa e le sfide che ci attenderanno.

Quello che si auspica in primo luogo è la predisposizione di veri e propri piani sulla comunicazione istituzionale sia per i tempi di emergenza che non, al fine di individuare soggetti professionisti capaci di veicolare nel modo più affine agli interlocutori il messaggio e recuperare il rapporto e la fiducia tra istituzioni, esperti, cittadini. Durante la pandemia abbiamo, infatti, potuto osservare un'enorme quantità di informazioni provenienti sia dalle molteplici istituzioni coinvolte a vari livelli sia da esperti, diffuse in modo spasmodico, poco coordinato e privo di coerenza.

Si tratta di pianificare il futuro privilegiando la qualità rispetto alla quantità di informazioni che rischiano solo di creare disorientamento e sfiducia.

In secondo luogo, le sfide che ci attendono richiederanno l'individuazione di un giusto bilanciamento tra tutela della salute pubblica e ripresa delle atti-

vità produttive e sociali, che inevitabilmente dovrà passare per una riorganizzazione, se non addirittura rivoluzione dei processi amministrativi che dovranno accompagnare il cittadino, coinvolgendolo proattivamente, verso una responsabilizzazione condivisa che disegni un contesto sociale moderno e sicuro.

Tali processi dovranno essere coadiuvati dalla formazione di conoscenze e competenze e dall'alfabetizzazione digitale e mediatica della pubblica amministrazione e dei cittadini, oggi ancora insufficiente. Solo in questo modo sarà possibile prevedere processi amministrativi digitali trasparenti e razionali, capaci di assumere decisioni in modo agile attraverso una comunicazione ed informazione, sia interna che esterna, efficace.

In una società dove le opportunità di contatto fisico e relazionale sono ridotte ai minimi termini, sarà proprio il messaggio e la comunicazione a giocare un ruolo primario. Proprio per questo sarà di fondamentale importanza investire sul patrimonio culturale, di competenze e conoscenze del cittadino, a tutti i livelli, al fine di renderlo in grado di recepire e comprendere i messaggi delle istituzioni e delle amministrazioni e capace di una maggiore partecipazione, così da recuperare quel rapporto di fiducia estremamente necessario perché le regole vengano rispettate e le istituzioni legittimate.

La comunicazione posta al centro, chiamerà giuristi, sociologi, economisti, esperti di tecnologie, e filosofi a plasmare quella che sarà la società del futuro.

Come abbiamo visto, il percorso evolutivo della funzione di comunicazione pubblica rispetto alle nuove tecnologie ha messo in luce da un lato una forte disomogeneità nell'applicazione dei nuovi paradigmi comunicativi soprattutto legati a i nuovi media e dall'altro il tema della qualità della comunicazione istituzionale sui social come momento di informazione e dialogo con il cittadino.

L'importanza della comunicazione di qualità sembra essere ormai un tema noto, basti pensare ai vari tentativi di introdurre linee guida come il *Vademecum* "Pubblica amministrazione e social media" di Formez del 2011, il libro *in progress* "Social media e PA, dalla formazione ai consigli per l'uso" del 2018 nonché dello stesso anno sul tema della scrittura sul web pubblico la "Guida al linguaggio della Pubblica amministrazione" a cura del Dipartimento per la trasformazione digitale e pubblicata on-line da AgID[78].

Una comunicazione di qualità è sufficiente a ricucire lo scollamento che negli anni si è venuto a creare tra istituzioni, Pubblica amministrazione e cittadino? È sufficiente a proteggere il cittadino da tutte le degenerazioni comunicative sopra descritte proprie dei social media e che rischiano di inquinare il dibattito pubblico?

La risposta non può che essere negativa, perché pur essendo di fondamentale importanza continuare ad insistere sulla qualità del messaggio è altresì necessario operare anche in altri ambiti.

In primo luogo, pare opportuno che le istituzioni continuino a mantenere alta l'attenzione sulle piattaforme social nelle mani dei grandi *Gatekeeper* per quanto riguarda temi sensibili come la protezione dei dati dei cittadini, la tutela della privacy, e tutta quella serie di valori democratici legati alla libertà di espressione che rischiano altrimenti di essere intaccati da un uso scorretto dei social.

Nonostante in molti abbiano concepito Internet come un ordinamento separato da quello reale, naturalmente refrattario ed immune per le sue caratteristiche intrinseche alle regole statali, pare oggi chiaro che un intervento da parte degli Stati sia sempre più auspicabile e non più procrastinabile a fronte, come abbiamo avuto modo di vedere, della progressiva coincidenza tra vita on-line ed off-line e della forte incidenza degli OTT nella vita pubblica, con tutto ciò che ne consegue. A ciò si è affiancata anche la difficoltà dei singoli Stati di porsi in relazione con i prestatori di servizi digitali che operano in uno spazio ambiguo, il cui statuto giuridico, in bilico tra dimensione privata e dimensione pubblica, pone sempre più la questione della natura di questi soggetti e del rapporto tra democrazia e potere.

Pare oggi chiaro che un eventuale intervento normativo volto a regolare i rapporti tra le piattaforme e gli utenti possa essere messo in campo unicamente da un soggetto sovranazionale quale l'Unione europea, la quale ha una visione ed un peso maggiore a livello internazionale. Ed anche gli sforzi compiuti da quest'ultima talvolta non sembrano essere sufficienti rispetto alle dinamiche globali in cui operano queste piattaforme che richiederebbero un intervento di respiro più ampio ma al momento del tutto utopico.

Gli interventi dell'Unione europea, sebbene apprezzabili, stanno faticando a dare i propri risultati. Si sono dimostrati poco efficaci a causa di iter e tempi di produzione normativa lenti rispetto ai tempi di evoluzione delle tecnologie e delle problematiche ad esse collegate (si pensi per esempio al lungo iter che ha accompagnato la produzione e l'adozione del Regolamento 2016/679 GDPR). Inoltre, la tendenza è stata quella di considerare questi temi alla stregua di problematiche antitrust dando vita ad una legislazione incentrata su logiche di mercato anziché sui diritti del cittadino.

Infatti, la legislazione così prodotta è caratterizzata da una forte attenzione agli aspetti tecnici delle

piattaforme e delle soluzioni da mettere in campo rischiando una veloce obsolescenza e perdendo di vista quello che dovrebbe essere il fine ultimo: la tutela dei diritti.

Da un lato sarebbe auspicabile una legislazione guidata da una strategia meno legata agli aspetti tecnologici e in grado, quindi, di produrre norme più resilienti rispetto alle veloci trasformazioni del mondo digitale, dall'altro è sempre più evidente come sia assolutamente necessaria una maggiore sinergia tra i tecnici del diritto ed i tecnici informatici al fine di effettuare un corretto bilanciamento tra i diritti in gioco e le soluzioni tecniche da mettere in campo.

Scelte che non tengano conto delle implicazioni sulla sfera dei diritti derivanti dall'applicazione di particolari soluzioni tecnologiche o viceversa scelte che non tengano conto delle implicazioni sul mercato di soluzioni strettamente giuridiche, rischiano nel migliore dei casi di essere poco efficaci.

Paradossalmente una eccessiva normazione di questo settore che non tenga in debito conto questi aspetti rischia di polarizzare ulteriormente un mercato già afflitto da pesanti forme di oligopolio, innalzando in maniera significativa la soglia di ingresso in questo settore da parte di attori emergenti i quali spesso si presentano con forme societarie embrionali (si pensi alle start up) prive degli strumenti organizzativi ed economici necessarie a rispettare i requisiti previsti dalle normative.

E questo non fa altro che spostare ulteriormente il rapporto di potere tra Pubbliche amministrazioni ed OTT in favore di questi ultimi, i quali oltre che essere unici depositari del codice e dei servizi ormai necessari al cittadino per svolgere la propria vita a cavallo tra quella reale e quella digitale, sono sempre più il mezzo attraverso il quale le istituzioni e le Pubbliche amministrazioni svolgono le proprie funzioni estrinsecando il loro potere.

L'attività normativa è sicuramente necessaria visto il ruolo di piattaforme di pubblica utilità che i social media hanno assunto, loro malgrado, nel tempo. Tuttavia, a causa dei lunghi tempi di produzione normativa, gli OTT si sono trovati spesso ad operare in un regime di discrezionalità su tematiche che invece avrebbero richiesto l'intervento delle istituzioni nazionali ed europee.

È quindi auspicabile a fianco dell'attività legislativa un dialogo costante ed un operato sinergico tra le istituzioni e le grandi piattaforme social al fine di guidarne l'evoluzione verso un sistema in cui la loro natura di piattaforma di marketing risulti distinta e ben distinguibile dalla loro natura di piattaforma di pubblica utilità al fine di delineare un futuro sostenibile per l'informazione on-line.

Così come durante il processo di produzione normativa i social media sono chiamati a partecipare alla discussione portando importanti contributi, così sarebbe altrettanto importante che le istituzioni contribuissero ai processi evolutivi delle piattaforme quando questi incidano sui temi di interesse pubblico.

In assenza di tutto ciò le piattaforme, di fronte a fenomeni come fake news ed *hate speech* i quali con il tempo hanno messo fortemente a rischio l'appetibilità dei propri servizi, si sono trovate costrette ad arginare tali fenomeni con soluzioni come sistemi di pre e post moderazione o come abbiamo visto più di recente con l'istituzione del "Tribunale di Facebook", rischiando così di dar vita a forme di censura o di discriminazione ergendosi a giudici di informazioni ed opinioni, andando ad intaccare non solo tra le altre la libertà di espressione ma anche il sistema democratico[79].

Queste attività poste in essere in autonomia dai gestori delle piattaforme social non possono che basarsi esclusivamente sui principi economici e mancano totalmente di un bilanciamento tra appetibilità di mercato e difesa dei diritti dell'utente. È per questo che è importante che su temi sensibili l'evoluzione di queste piattaforme avvenga in maniera sinergica con le istituzioni che invece debbono farsi garanti del rispetto di tali diritti.

Un possibile ambito di sinergia potrebbe essere quello della certificazione di notizie o di estratti di esse per combattere la diffusione delle fake news. Attraverso l'utilizzo di tecnologie *Blockchain*, che hanno come fondamento il concetto di fiducia distribuita, sarebbe possibile ad esempio implementare dei processi di *fingerprinting* dei contenuti (testuali, immagini o video), censire le "impronte" all'interno della *Blockchain* in modo che risultino inalterabili e pubblicamente consultabili, ed in seguito permettere alle varie piattaforme social di automatizzare il processo di verifica della provenienza delle fonti. È importante notare che tale processo di *fingerprinting* è rappresentato da un insieme di algoritmi pubblici che possono operare ad un semplice livello formale ovvero creando un'impronta del contenuto di un testo alla lettera oppure ad un livello semantico ovvero andando ad analizzare l'argomento trattato, il tono della trattazione ed il significato del testo. Se nel primo caso, una citazione che riportasse un contenuto privo di una congiunzione o di una punteggiatura risulterebbe alterata e quindi non conforme, poiché l'impronta calcolata con il medesimo algoritmo a partire da questo nuovo testo risulterebbe diversa da quella censita nella *Blockchain*, nel secondo caso ciò avverrebbe solo se la citazione stravolgesse il senso semantico della fonte.

In questo caso risulta evidente come si possa spaziare da un algoritmo poco costoso ma anche poco efficace, ad uno maggiormente costoso ma più efficace e che quindi sia necessario operare un bilanciamento tra gli obiettivi che si vogliono perseguire (l'efficacia dell'algoritmo) e la sua sostenibilità da un punto di vista di mercato, affinché le piattaforme siano spinte ad adottarlo.

Fine ultimo dell'implementazione di queste tecnologie potrebbe essere quello di limitare forme di censura privata messe in campo dalle piattaforme con sistemi di pre e post moderazione nel tentativo di porre un freno al dilagare di forme di disinformazione in assenza di soluzioni alternative da parte delle istituzioni, di permettere altresì a queste ultime di veicolare il proprio messaggio in un ambiente dove la comunicazione di qualità sia maggiormente riconoscibile ed infine di consentire ai cittadini di ricostruire quella gerarchia delle fonti, oggi venuta meno con i nuovi paradigmi comunicativi, e meglio orientarsi nel panorama informativo.

È anche di fondamentale importanza sottolineare come attraverso questo approccio non si vada a cristallizzare una verità certificata dalle istituzioni oppure dai soggetti privati, ma piuttosto a fornire all'utente un potente strumento di verifica delle fonti a supporto di una formazione critica delle opinioni, attraverso un sistema volto ad evidenziare la provenienza di una affermazione ed a certificare l'assenza di manipolazioni.

Risulta quindi chiaro come, accanto all'attività normativa nonché ad una auspicata maggiore sinergia tra istituzioni e piattaforme social, sia fondamentale avviare un percorso di alfabetizzazione mediatica volto a rendere sempre più consapevoli i cittadini delle loro azioni on-line e a sviluppare un pensiero critico importante nel contrasto alla disinformazione e nella formazione di una opinione pubblica sana.

Se infatti oggi le istituzioni scolastiche con il supporto della famiglia forniscono all'individuo gli strumenti necessari ad affrontare le sfide del mondo reale, altrettanto non può dirsi con riguardo al mondo digitale.

Spesso le istituzioni scolastiche confondono l'alfabetizzazione mediatica con quella informatica e si concentrano sull'utilizzo degli strumenti e delle tecnologie, ignorando in gran parte l'importanza dello sviluppo del pensiero critico, della capacità di discernere notizie false o incomplete, del verificare le fonti, del valutare le conseguenze delle proprie azioni on-line (si pensi a fenomeni quali cyberbullismo, *hate speech*, *revenge porn* etc.). Anche la famiglia risulta oggi del tutto inadatta ad affrontare queste tematiche in quanto a sua volta priva di una adeguata formazione, finendo per passare dall'essere parte della soluzione a divenire parte del problema.

In assenza di una adeguata alfabetizzazione mediatica che includa anche temi legati all'etica del vivere civile, i cittadini della rete somigliano sempre più ai bambini nell'isola del "Signore delle Mosche"[80], innocenti e privi di sovrastrutture, ma anche privi dei mezzi per creare una società sana, guidati unicamente da istinti primordiali.

Dell'importanza di questi aspetti sembra aver assunto maggiore consapevolezza anche la Commissione europea soprattutto in relazione ai fenomeni di disinformazione, la quale nel Piano d'azione per la democrazia in Europa del dicembre del 2020 ha sottolineato l'importanza di dar vita a nuovi progetti di alfabetizzazione che vedano coinvolti gli istituti di istruzione superiore, le organizzazioni della società civile ed i giornalisti.

Tuttavia, per quanto lodevole, si tratta di un intervento già tardivo e che se non attuato tempestivamente rischia di essere poco incisivo vista la velocità con la quale i mezzi di comunicazione sul web evolvono.

Il paradosso al quale siamo giunti nell'arco di neanche un decennio è quello che vede le istituzioni e Pubbliche amministrazioni, in mancanza di una alternativa, rivolgersi ai soggetti privati al fine di rendere possibile il servizio pubblico ed intercettare ed avviare un dialogo con il cittadino ormai presente prevalentemente su queste piazze. Si è venuto così a creare un rapporto di vera e propria dipendenza delle istituzioni e delle Pubbliche amministrazioni nei confronti degli OTT che rischia di alterare i rapporti di potere, dove, come abbiamo visto sono i *Gatekeeper* a stabilire le condizioni contrattuali di fornitura del servizio, in una sorta di "prendere o lasciare".

7. È possibile una piattaforma social di pubblica utilità?

Se come abbiamo visto, la convivenza sui social media delle istituzioni e delle Pubbliche amministrazioni con tutte le altre fonti di produzione delle informazioni è resa particolarmente difficile dalle caratteristiche intrinseche delle piattaforme, dalla loro natura privatistica e dai loro algoritmi, viene da chiedersi se non sia utile una riflessione circa l'opportunità di realizzare una piattaforma social pubblica, federata a livello europeo e che tratti esclusivamente temi di pubblica utilità.

Ben lungi dall'idea di un "social di Stato", tale piattaforma dovrebbe proporsi come complementare alle attività di comunicazione che la Pubblica amministrazione, come abbiamo avuto modo di vedere, già

espleta sulle piattaforme social private, in un'ottica di multicanalità.

Ci si può d'altro canto chiedere se una piattaforma che si concentri su temi così specifici, abbandonando il generalismo tipico di piattaforme come Twitter e Facebook, calata nel contesto del mercato dell'informazione attuale, possa suscitare da parte dei cittadini l'interesse necessario a costituire una base di utenti sufficientemente solida per rendere efficace il paradigma di comunicazione social.

Osservando le recenti evoluzioni del mercato dell'informazione emerge come vi sia un progressivo allontanamento dal paradigma generalista e la ricerca da parte degli utenti di piattaforme che trattano temi specifici attraverso linguaggi particolarmente adatti alla loro trattazione. Si pensi ad esempio alle recenti acquisizioni di Instagram e Whatsapp da parte di Facebook, guidate dalla necessità di differenziare il bacino di utenti, soprattutto dopo aver registrato un notevole calo nel numero di utenti attivi proprio a favore di queste ultime piattaforme; o alla nascita di attori di rilievo come Linkedin divenuto il punto di riferimento per tutte le tematiche legate al mondo del lavoro[81].

I cittadini sembrano, quindi, pronti a recepire una piattaforma social che tratti temi specifici di pubblica utilità e potrebbero trovare particolarmente appetibile una informazione di qualità su temi istituzionali, disintermediata e fruibile in modo semplice e intuitivo attraverso quei paradigmi che hanno decretato il successo dei social media.

Se è vero quindi che una tale piattaforma potrebbe trovare una propria collocazione nel panorama dei social media non ci resta che mettere in luce le sue potenziali caratteristiche ed i benefici che ne potrebbero derivare.

In primo luogo, il codice e gli algoritmi relativi a questa piattaforma, pur rimanendo proprietari, dovrebbero essere pubblicamente consultabili nel classico stile delle applicazioni open source. Questo consentirebbe di garantire una maggiore trasparenza riguardo alle tematiche relative alla privacy, al trattamento del dato ed agli algoritmi di ranking applicati.

Inoltre, ciò permetterebbe di superare il disallineamento tra i termini di servizio delle piattaforme e le policy interne ed esterne di utilizzo da parte delle Pubbliche amministrazioni e delle istituzioni. In presenza infatti di una piattaforma social pubblica, gli obbiettivi perseguiti non sarebbero più guidati da logiche di mercato ma da logiche di pubblico servizio.

Il fatto che tali policy discendano naturalmente dai termini di servizio della piattaforma, ed evolvano costantemente con essi essendo il prodotto dei medesimi processi decisionali e dei medesimi principi fondanti, ridurrebbe drasticamente la dipendenza della comunicazione pubblica da sistemi di moderazione privati.

Anche i sistemi di moderazione potrebbero beneficiare di una maggiore trasparenza tanto negli algoritmi utilizzati, quanto nella pubblicità delle decisioni assunte, e questo sembra essere in linea con l'orientamento del legislatore europeo (in particolare nel *digital service act*) che da tempo auspica una maggiore chiarezza nei principi che guidano la moderazione dei contenuti sulle piattaforme social attraverso l'introduzione di un sistema di *notice and take down*.

Attraverso l'integrazione con i protocolli di sistemi di autenticazione Spid e CIE, la piattaforma permetterebbe di superare i problemi legati all'assenza di una identificazione certa dell'utente tipica dei social media privati. Questo consentirebbe innanzitutto di garantire la riconoscibilità dei soggetti istituzionali, non solo a livello di ente, ma addirittura a livello di operatore, andando a rendere ben distinguibile il messaggio istituzionale e facilitando la ricostruzione delle fonti da parte del cittadino.

D'altro canto, ciò consentirebbe anche l'introduzione di un canale di comunicazione certificato tra il cittadino e la Pubblica amministrazione in cui anche la comunicazione di tipo funzionale potrebbe trovare collocazione. Le richieste del cittadino, infatti, grazie alla sua identificazione certa potrebbero essere inoltrate alla Pubblica amministrazione e protocollate, ed avviare un iter presso l'ufficio competente.

Oggi il cittadino o il professionista si trovano a comunicare con la Pubblica amministrazione attraverso un sistema farraginoso caratterizzato da una serie di strumenti e registri di linguaggio disomogenei. Anche quando i servizi vengono erogati in via digitale questo avviene attraverso sistemi personalizzati, diversi da amministrazione ad amministrazione e che vedono obbligano il cittadino ad un cambio di paradigma rispetto a quello a cui è abituato dalle piattaforme commerciali, ponendolo spesso in difficoltà. Attraverso l'utilizzo, invece, di una piattaforma che riporti il modello comunicativo verso un paradigma social, più congeniale all'utente, in un ambiente controllato, dove viene certificata l'identità degli attori coinvolti, dove l'interazione è sottoposta ad auditing ed è sempre disponibile per la consultazione, è possibile tentare di raggiungere un modello di omogeneità nell'accesso alla pletora di servizi frammentati della Pubblica amministrazione non solo a livello nazionale ma anche, attraverso un insieme di sistemi statali federati, a livello europeo.

A ciò si potrebbe affiancare anche la possibilità, se pensiamo ad una comunicazione di promozione dell'immagine della Pubblica amministrazione o socia-

le, di delegare tali attività a soggetti privati legittimati a veicolarle tramite la piattaforma social della Pubblica amministrazione, grazie proprio a sistemi di identificazione certa.

Per garantire l'efficacia della piattaforma è sicuramente di fondamentale importanza lo scambio di dati tra le Pubbliche amministrazioni e tra queste ed il cittadino. Come già ampiamente discusso un protocollo di interscambio di dati aperto ed efficiente quale l'open data consentirebbe di far confluire le numerose banche dati disseminate sul territorio in un unico flusso informativo a disposizione delle Pubbliche amministrazioni e attraverso queste degli enti, dei cittadini, delle imprese e dei professionisti.

L'introduzione di un flusso dati al di fuori del pubblico dominio richiede tuttavia una particolare attenzione in termini di sicurezza e trattamento del dato. Senza scendere nel dettaglio, in questa sede, delle tematiche relative alla privacy e al trattamento del dato, in questo caso dovrebbero essere escluse tutte le finalità di trattamento orientate ai fini di marketing o di propaganda, tipiche delle piattaforme private, aprendo la possibilità di adottare sistemi di *sentiment analysis* e *machine learning* al fine di migliorare i servizi delle Pubbliche amministrazioni e monitorare l'impatto delle scelte da queste effettuate.

Quello appena descritto è un modello comunicativo social di pubblica utilità epurato da gran parte di quegli elementi che rendono i social media poco adatti, come abbiamo visto, ad alcune tipologie di comunicazione istituzionale.

8. La comunicazione istituzionale al centro della trasformazione digitale delle Pubbliche amministrazioni

Viene dunque da chiedersi quali possano essere i benefici derivanti dall'adozione di un tale modello di comunicazione all'interno dei processi amministrativi e dei servizi erogati dalle Pubbliche amministrazioni.

La piattaforma social appena descritta potrebbe quindi fungere da punto di accesso unico ai servizi delle Pubbliche amministrazioni andando a dare attuazione all'art. 64-*bis* CAD secondo cui le pubbliche amministrazioni sono tenute a rendere fruibili i propri servizi in rete, in conformità alle regole tecniche di cui all'articolo 71, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica.

A ben vedere si tratterebbe non solo di mettere a disposizione dei cittadini un unico punto di accesso ma anche di modificare profondamente le modalità di interazione con i servizi delle Pubbliche amministrazioni, passando dall'ormai tradizionale modello del portale ad un modello social con il quale l'utente ha maggiore familiarità.

Il tradizionale form presente sui portali (per esempio per la richiesta di servizi scolastici o quelli dedicati all'apertura di pratiche per i professionisti e gli imprenditori), caratterizzato da una elevata complessità, scarsa chiarezza e flessibilità, dalla presenza di numerosi voci opzionali, spesso corredato da voluminosi manuali di istruzioni, viene qui sostituito da una più familiare ma non meno efficace chat multimediale, nella quale sono coinvolte non solo figure umane (impiegati degli uffici competenti, professionisti, cittadini) ma anche algoritmi (c.d. *chat bot*) in grado di analizzare la conversazione e coinvolgere i servizi digitali delle Pubbliche amministrazioni dove necessari.

Pensiamo ad esempio ad un *chat bot* specifico per la protocollazione, il quale ad ogni documento, immagine o video postato sulla chat intervenga inviando il contenuto al servizio di *backend* di protocollazione della Pubblica amministrazione e restituisca in chat il numero di protocollo ottenuto, oppure ad un *chat bot* che conosca tutti i passi necessari per istruire una pratica e rilevando la chiusura di una specifica richiesta presenti in chat i requisiti per il passo successivo del processo. Questo consentirebbe anche di disegnare dei processi guidati (c.d. *Wizard*) in cui l'interazione avviene attraverso i paradigmi tipici della comunicazione sociale ed in cui l'interscambio di dati tra le Pubbliche amministrazioni permetterebbe di richiedere al cittadino o al professionista solo la quantità minima di dati necessaria non ancora in loro possesso.

Merita infine precisare che tale modalità di interazione rispetterebbe i requisiti di sicurezza e riservatezza necessari trattandosi di una comunicazione privata tra gli aventi interesse, pur mantenendo tutti i criteri di tracciabilità necessari a garantire la trasparenza e l'accountability dei processi amministrativi.

La forte accelerazione nell'utilizzo di servizi digitali della Pubblica amministrazione impressa dalla crisi da Covid-19 ha reso evidente un profondo scollamento tra il modello di interazione e di fruibilità fornito dai servizi offerti dall'amministrazione e quello auspicato dagli amministrati.

Oggi in presenza di una situazione di crisi, una piattaforma come quella sopra descritta avrebbe potuto fornire un valido ausilio al cittadino spesso frustrato dall'impossibilità di accedere ai servizi in presenza e, anche laddove siano stati messi a disposizio-

ne servizi digitali, dalla difficoltà di portare a termine con successo una richiesta a causa della complessità e scarsa funzionalità dei modelli di interazione.

Ma il modello proposto è fantascienza?

In particolare, un progetto come *Slack*[82] dimostra come un processo collaborativo costruito intorno ad un modello comunicativo social, simile a quello appena descritto, possa risultare efficace ed efficiente.

Oggi *Slack* fornisce un ambiente di comunicazione multicanale e multimediale che permette, grazie all'integrazione di software leader di mercato e app personalizzate (si pensi a Google drive, Zoom, Salesforce, Microsoft outlook), di gestire flussi di lavoro in modo collaborativo, garantendo elevati standard di sicurezza ed un alto livello di automazione dei processi. La sua rapida diffusione soprattutto in ambienti altamente innovativi e caratterizzati da un elevata complessità, come lo sviluppo software, ha chiaramente mostrato da un lato i vantaggi di un simile approccio basato sul modello di comunicazione sociale, dall'altro l'estrema appetibilità del modello di distribuzione del software Saas (*Software as a service*)[83] che permette di utilizzare tecnologie molto complesse delegando la gestione di queste tecnologie a soggetti terzi.

Un sistema caratterizzato da un modello comunicativo che sfrutti i paradigmi social e una organizzazione dei processi di lavoro non dissimile da *Slack*, potrebbero confluire nella applicazione IO.it, che sta diventando un punto di accentramento dei vari servizi delle Pubbliche amministrazioni.

Il progetto IO.it[84] prende le mosse dalla necessità di porre il cittadino al centro dei processi produttivi e di comunicazione della Pubblica amministrazione, offrendo un punto di accesso unico e facilmente utilizzabile alla pletora di servizi fino ad oggi estremamente frammentati e disomogenei. Attraverso l'utilizzo di integrazioni con le banche dati dei vari enti, con i servizi di pagamento PagoPA e con i sistemi di identificazione Spid e CIE, esso si pone l'obiettivo di fornire una applicazione integrata e fruibile in modo semplice attraverso gli stilemi tipici delle applicazioni mobili. Seppur ancora in versione beta l'applicazione, in particolare durante il periodo di pandemia, si è rivelata particolarmente utile nel processo di alfabetizzazione digitale dei cittadini, e nel favorire l'adozione di tecnologie strategiche per il piano innovativo nazionale quali PagoPA e Spid.

Sebbene si tratti di un progetto di ispirazione nazionale, non è da escludersi che questo in caso di successo, possa ispirare anche l'operato di altri paesi europei.

Ecco che un intervento di tipo federativo dell'Unione europea potrebbe creare i presupposti per una completa interoperabilità tra i vari sistemi nazionali, con grande beneficio dei cittadini europei che potrebbero fruire di tutti i servizi di cui hanno bisogno su tutto il territorio comunitario.

Un ultimo aspetto da prendere in considerazione riguarda l'estrema complessità delle tecnologie alla base di questi sistemi. Visti gli elevati costi di gestione degli strumenti necessari a garantirne il funzionamento si sarebbe portati a pensare che soltanto i grandi OTT (come Amazon o Google) abbiano la capacità di realizzare ed operare infrastrutture così complesse, tuttavia, negli ultimi anni i maggiori cloud provider hanno iniziato ad offrire tali tecnologie in modalità completamente gestita, con tariffe flessibili e vantaggiose. Oggi è possibile per piccole aziende, e quindi anche per le Pubbliche amministrazioni, realizzare sistemi innovativi di grandi dimensioni a costi incrementali.

Se il tema della gestione dei dati dei cittadini su piattaforme di soggetti privati è stato già a lungo dibattuto ed ha in parte trovato una soluzione, tanto che AgID ha stilato una lista di cloud provider qualificati cui le Pubbliche amministrazioni possono rivolgersi per acquistare servizi informatici[85], si pone tuttavia un problema, più che di costi e di efficienza, di affidabilità dei soggetti privati che forniscono le infrastrutture.

Il recente caso che ha coinvolto l'applicazione social americana *Parler*, di chiaro stampo repubblicano ed il colosso del *cloud Amazon*, che ha visto quest'ultimo interrompere l'erogazione dei servizi cloud al social in seguito agli eventi di *Capitol Hill* del 6 gennaio 2020, ha mostrato come esista e sia tangibile il rischio che impostando tutta la propria strategia di innovazione e tutti i propri servizi su infrastrutture fornite da soggetti privati, si giungerebbe ad una inversione dei rapporti di potere tra Stato e OTT dando vita ad una condizione di dipendenza del primo rispetto al secondo e mettendo a rischio l'erogazione di servizi di pubblica utilità fondamentali per il funzionamento del sistema paese.

Sebbene in Italia sia possibile riscontrare la presenza di progetti pionieristici di alcune Regioni (in particolare la Regione Friuli Venezia Giulia con il sistema cloud EELL e la Regione Toscana con il *Tuscany Internet eXchange* c.d. TIX)[86] le quali hanno attivato un'infrastruttura per la fruizione di servizi cloud di tipo Iaas, è da rilevare come la complessità e le dimensioni dei sistemi necessari a sostenere una app Io.it che comprenda anche le funzionalità prospettate richieda un investimento statale se non addirittura comunitario.

Anche in questo caso i singoli interventi statali potrebbero beneficiare della supervisione della Co-

munità europea che potrebbe fornire gli schemi di interoperabilità fra i vari cloud nazionali in modo da garantire lo sviluppo di un fiorente mercato digitale europeo all'interno del quale le amministrazioni possano condividere tecnologie ed infrastrutture.

Proprio in questa direzione pare muoversi il progetto Gaia-X[87] sorto sulla base di accordi Francia – Germania, ma presto allargatosi anche ad altri Stati membri. Tale progetto mira a costituire un ecosistema sicuro e federato che abbracci i più alti standard di sovranità digitale ma al contempo promuova l'innovazione tecnologica, sviluppando requisiti comuni per un'infrastruttura del dato aperta, trasparente ed in grado di connettere tutti i paesi europei.

È alla luce di tale contesto che nelle ultime settimane il Ministro per l'innovazione tecnologica e la transizione digitale Colao ha annunciato di voler avviare la creazione di un Polo Strategico Nazionale (PSN) per la realizzazione di un cloud nazionale per la Pubblica amministrazione che sarà operativo a partire dal 2022, ispirato al modello di cloud nazionale Francese.

Il ministro ha dichiarato che l'infrastruttura promossa dalla Presidenza del Consiglio prevederà la possibilità per le amministrazioni di usufruire di efficienti servizi cloud esclusivamente accessibili alla Pubblica amministrazione o ibridi, economici e scalabili facilmente, a fronte di una rigorosa ed omogenea classificazione delle tipologie di dati da conservare e delle caratteristiche di sicurezza e protezione richieste ai fornitori[88].

Per la realizzazione dell'infrastruttura fisica e tecnologica del cloud nazionale è previsto l'avvio di un partenariato pubblico-privati, sulla quale basare servizi e piattaforme del settore pubblico e privato. I *data center* saranno collocati in Italia e a controllo italiano a garanzia della sicurezza dei dati connessi all'esercizio di funzioni essenziali dello Stato e dovranno rispettare i requisiti di qualità, sicurezza, performance e portabilità stabiliti da AgID.

Le dichiarazioni del Ministro sembrano mostrare la volontà del Governo di virare verso scelte di policy che pongano un argine all'ingresso delle *Big tech* (per la maggior parte straniere) nella realizzazione del cloud nazionale, soprattutto per quanto concerne il trattamento del dato. Tuttavia, nonostante l'iniziativa sia lodevole e costituisca un grosso passo in avanti per il nostro paese, resta da capire quali saranno i criteri per la scelta dei provider, e soprattutto come verranno custoditi e trattati i dati degli amministrati, al fine di evitare proprio quell'inversione dei rapporti di potere e di progressiva dipendenza OTT-Stato, dei quali abbiamo parlato.

9. Conclusioni: verso una riforma della comunicazione pubblica?

Come abbiamo visto, oggi la comunicazione pubblica è regolata prevalentemente dalla l. 150/2000 che se da un lato mostra una sostanziale inadeguatezza ad affrontare i modelli comunicativi moderni, dall'altro ha faticato a trovare una piena e concreta attuazione nel corso degli anni.

Tuttavia, nonostante le difficoltà applicative e le prevedibili resistenze burocratiche, la l. 150/2000 ha avuto un ruolo fondamentale nel ribaltare il modo in cui è concepito da sempre il rapporto tra Pubblica amministrazione e cittadino tanto da introdurre il mantra "la trasparenza è la normalità, il segreto l'eccezione" nel rispetto di quanto affermato dall'art. 97 Cost.

Il 9 gennaio 2020 si è insediato presso la Funzione pubblica un tavolo di lavoro voluto dal ministro per la PA Fabiana Dadone con lo scopo di occuparsi di una riforma complessiva di una normativa e della contrattualistica relative alla comunicazione delle Pubbliche amministrazioni e fornire al contempo indirizzi per una social media policy nazionale.

L'iniziativa si inserisce nel più ampio quadro della partecipazione italiana all'*Open Government Partnership* (OGP) volta a promuove negli oltre 70 Stati aderenti, l'apertura del governo e dell'amministrazione attraverso l'uso di open data, la trasparenza, la partecipazione dei cittadini, l'accountability degli amministratori, l'uso dei servizi digitali e le competenze digitali nelle amministrazioni e tra i decisori pubblici, sottolineando ancora una volta lo stretto legame tra comunicazione pubblica e trasparenza.

Al gruppo di lavoro hanno partecipato le principali organizzazioni della comunicazione, del giornalismo, e delle professioni digitali, nonché Università, associazioni civiche e rappresentanze di Regioni e Comuni (Associazione comunicazione pubblica, Formez P.A., Ordine dei giornalisti, Fnsi, Ferpi, le Università, PaSocial, Agcom, Associazioni civiche OGP, Anci, Conferenza delle Regioni).

Il 16 giugno 2020, il Gruppo di lavoro su Riforma della comunicazione pubblica e social media policy nazionale ha consegnato nelle mani della Ministra Fabiana Dadone una proposta operativa in 10 punti per una riforma della comunicazione pubblica ed un documento di indirizzo, realizzato da Sergio Talamo, dove vengono evidenziati i motivi che hanno frenato la piena e compiuta realizzazione degli obbiettivi della l. 150/2000 ed i nuovi obbiettivi di riforma (si tratta della c.d. l. 151 per evidenziare la volontà di un superamento delle logiche della vecchia l. 150/2000).

La proposta per la riforma della comunicazione ha quali principali obiettivi quello di mettere il cittadino al centro delle scelte comunicative dell'amministrazione; estendere i principi di trasparenza non solo a quella legata ai principi di anticorruzione ma anche alla trasparenza legata ai processi decisionali (accountability); l'uso professionale dei social e delle nuove tecnologie allo scopo di instaurare un rapporto diretto, interattivo ed in tempo reale con il cittadino nei luoghi virtuali in cui effettivamente opera ed interagisce con il mondo esterno; costituire un'unica area integrata e digitale di comunicazione stampa e servizi al cittadino che presenti però profili distinti: il giornalista pubblico (chiamato alla redazione delle notizie ed al trattamento delle informazioni e rapporti con i media), lo specialista della comunicazione pubblica (che si occupa di contatti con il pubblico, gestione dell'accesso civico finalizzato all'accountability; analisi della soddisfazione del cittadino; campagne di comunicazione ed organizzazione di eventi; comunicazione interna), social media manager (incaricato di gestire la comunicazione di tipo social prodotta dall'Ufficio unico).

Sebbene risulti lodevole l'intento di proporre una riforma della comunicazione pubblica ormai divenuta necessaria da anni, auspicando soluzioni già in parte illustrate nella nostra trattazione, questa pare tuttavia avulsa da una strategia più ampia che ponga la comunicazione pubblica e quindi il rapporto con il cittadino al centro del processo di digitalizzazione delle Pubbliche amministrazioni e dei servizi da esse erogati.

Tale proposta sembra orientata unicamente ad aggiornare il linguaggio comunicativo delle Pubbliche amministrazioni secondo i nuovi paradigmi imposti dal mercato dei social media, attraverso l'introduzione di figure *ad hoc*, concentrandosi prevalentemente sulla comunicazione pubblica e sull'informazione che oggi avviene attraverso l'Ufficio stampa e l'URP in ottica di comunicazione come servizio.

Come abbiamo visto, tuttavia, la comunicazione permea tutti i processi della pubblica amministrazione in modo trasversale ed assurge al ruolo di vera e propria funzione amministrativa. È chiaro quindi come una riforma che affronti la questione solo da un punto di vista di quelle declinazioni della comunicazione istituzionale adatte ad essere veicolata tramite i social media, escludendo ad esempio la comunicazione interna e quella funzionale, ha una efficacia molto circoscritta e rischia di presentare al cittadino una Pubblica amministrazione ancora troppo burocratizzata e lenta, afflitta da servizi legati a modelli di interazione superati, non al passo con le innovazioni tecnologiche riscontrate sul mercato.

Una presenza di qualità delle Pubbliche amministrazioni sui social, pur fornendo sicuramente un presidio importante contro fenomeni quali fake news, discorsi d'odio etc. non è da sola sufficiente a realizzare quell'idea di amministrazione trasparente, compartecipata ed efficiente che costituisce l'obiettivo dei processi di ammodernamento della Pubblica amministrazione e non è da sola in grado di creare i presupposti per l'ecosistema mediatico necessario a dar vita ad una opinione pubblica di qualità.

Infatti, se come abbiamo visto il modello comunicativo social è frutto di una profonda trasformazione della società in una "società informazionale" che fa dell'informazione il prodotto principale dei propri processi e della comunicazione il mezzo di scambio di tale prodotto, è allora necessario ridisegnare tutti i processi amministrativi proprio intorno alla comunicazione.

È il processo stesso di ammodernamento e digitalizzazione delle Pubbliche amministrazioni che deve plasmarsi intorno a quel paradigma comunicativo sociale oggi divenuto cardine della società, garantendo in questo modo *by design* la trasparenza ed il coinvolgimento diretto del cittadino nei processi decisionali, dove anche la comunicazione interna della PA finisce per divenire una declinazione della comunicazione con il cittadino condividendone il linguaggio, la forma, gli obbiettivi.

Ma tali ambiziosi obiettivi non possono essere raggiunti affidandosi ad infrastrutture e servizi privati forniti da terze parti, ma unicamente mantenendo quella sovranità digitale che oggi è possibile raggiungere solamente attraverso la cooperazione e la federazione tecnologica tra Stati che solo un soggetto come l'Unione europea può garantire.

In questo senso una piattaforma social di pubblica utilità, come sopra descritta, di proprietà degli Stati, integrata profondamente nei processi digitali delle Pubbliche amministrazioni e federata attraverso l'intervento unificatore dell'Unione europea, potrebbe aiutare a colmare la distanza venutasi a creare tra amministratori ed amministrati e a generare un ambiente mediatico in grado di garantire processi democratici sani.

Ecco che proprio grazie alla riprogettazione dei servizi della Pubblica amministrazione intorno al concetto di comunicazione, la trasparenza diviene accessibilità: non solo il dato è disponibile al cittadino, ma questo viene arricchito di un valore semantico che rende i dati interconnessi e navigabili, permettendogli non solo di accedere al dato ma anche di comprenderne il significato. Non è sufficiente infatti pubblicare un flusso continuo di dati e notizie riguardanti le attività svolte dalle Pubbliche amministrazioni, ma

è necessario dare al cittadino gli strumenti per verificare, confrontare e comprendere le informazioni con cui quotidianamente entra in contatto.

In questo senso, è sicuramente passo in avanti l'iniziativa con la quale AgID ha varato il nuovo portale di ricerca dati.gov.it[89], che ha l'obbiettivo di aggregare le numerose fonti open data delle Pubbliche amministrazioni, fornendo un unico punto di accesso centralizzato per eseguire ricerche in modo semplice e intuitivo.

Tutto ciò costituisce un primo contributo verso una maggiore accessibilità dell'informazione al cittadino, venendo meno la necessità di conoscere l'ubicazione delle singole banche dati (per es. siti Internet di Ministeri, enti locali o altri enti pubblici) e le specifiche modalità di interazione con ciascuna di esse. Tuttavia, tale strumento risulterebbe enormemente più efficace se integrata all'interno dei servizi delle Pubbliche amministrazioni anziché in un portale separato.

Ciò consentirebbe di evitare una perdita di contesto ogni volta che il cittadino, il professionista o l'impresa si trovino a dover reperire o verificare delle informazioni (si pensi per esempio durante la presentazione di una pratica la necessità di reperire l'Ufficio preposto o informazioni di contatto o ancora reperire il testo di una norma legata al servizio di cui si sta usufruendo).

Altresì è da notare come, in modo del tutto analogo a quanto fatto dai motori di ricerca agli albori dell'Internet, l'indicizzazione dei contenuti avvenga secondo un criterio formale, permettendo di ricercare esclusivamente informazioni di cui si conosca già parzialmente il contenuto, secondo il noto paradigma della ricerca per "parola chiave".

Come abbiamo visto tale modalità di indicizzazione, sebbene permetta di centralizzare l'accesso ai dati, non consente una organizzazione ontologico-semantica del dato, rendendo meno espressiva la ricerca e meno comprensibili i risultati. Mancano sostanzialmente quelle relazioni tra i dati che li rendono fruibili da una società informazionale il cui modello comunicativo, come visto, è basato sul concetto di rete.

È quindi chiaro che vi sia l'esigenza di centralizzare l'accesso ai servizi della Pubblica amministrazione e di creare una maggiore integrazione tra di loro, anche utilizzando gli strumenti e le tecnologie già consolidati sul mercato dai grandi attori del web (si pensi alla *machine learning* e agli algoritmi di ranking). Oggi è possibile osservare come una applicazione come IO.it, sebbene in fase sperimentale, raccolga molte di queste sfide, fornendo al cittadino un unico punto di accesso a tutti i servizi della Pubbliche amministrazioni, integrato con sistemi di pagamento e di identificazione, fruibile attraverso un paradigma ormai consolidato come quello della *app mobile* e con un linguaggio ampiamente derivante da quello delle grandi piattaforme social. Questa applicazione potrebbe costituire l'embrione di una piattaforma più ampia, costruita intorno ai processi comunicativi, come quella da noi prospettata. Il nome stesso Io.it pare suggerire la volontà di costruire un ecosistema dove il cittadino è posto al centro.

E se quindi l'obbiettivo è quello di porre di nuovo il cittadino al centro dei processi democratici ed assurgere a quel modello di democrazia compartecipata in cui le decisioni sono frutto di una sinergia tra amministratore ed amministrato, è necessario da un lato fornire ai cittadini i mezzi tecnologici necessari a rendere effettiva tale partecipazione, e dall'altro avviare un processo di alfabetizzazione mediatica che fornisca al cittadino gli strumenti necessari alla formazione di un pensiero critico alla base della corretta formazione dell'opinione pubblica.

Ciò potrà avvenire solo se la comunicazione pubblica, ed in particolare quella istituzionale, punto cardine dei processi di trasformazione della Pubblica amministrazione in chiave digitale e faro per il cittadino nella nebbia mediatica costituita dai nuovi media, saprà evolversi verso il modello comunicativo sociale della nuova società informazionale perseguendo il bene pubblico e divenendo per quella via un esempio virtuoso nel panorama mediatico, spingendo gli stessi cittadini-utenti a pretendere il medesimo livello di tutela dai grandi attori del web.

Note

[1] Il Digital Economy and Society Index (DESI) per il 2020 colloca l'Italia al 25° posto fra i 28 Stati europei. Rispetto alla media dei paesi Ue, l'Italia registra significative carenze in relazione alle competenze digitali di base e avanzate. Solo il 42% delle persone di età compresa tra i 16 anni e i 74 anni possiede delle competenze digitali essenziali di base (la media europea si attesta intorno al 58%), e solo il 22% dispone di competenze digitali superiori a quelle di base (33% nella media Ue). Al di sotto degli standard europei è inoltre la percentuale di specialisti ICT rispetto alla forza lavoro complessiva. Il Report cittadini e ICT dell'Istat, invece, segnala che nel 2019, in Italia il 76,1% delle famiglie dispone di un accesso a Internet ed il 74,7% di una connessione a banda larga. Resta un forte divario digitale riconducibile a fattori generazionali e culturali. La quasi totalità delle famiglie con un minore dispone di un collegamento a banda larga (95,1%), mentre tra le famiglie composte da persone con più di 65 anni la quota si abbassa al 34%. Il divario digitale ancora molto esteso nel nostro paese incide anche sull'esercizio di alcuni diritti e libertà fondamentali quali l'accesso alle informazioni e la libera manifestazione del pensiero.

[2] L. Mazzoli, *Il patchwork mediale. Comunicazione e informazione tra media tradizionali e media digitali*, Franco Angeli, 2017.

[3]J. Lazer, M. Baum, Y. Benkler et al., *The science of fake news. Addressing fake news requires a multidisciplinary effort*, in "Sciencemag.org", 2018, n. 6380.

[4]Per quarta rivoluzione industriale si intende la crescente compenetrazione tra mondo fisico, digitale e biologico veicolata dalle nuove tecnologie (si pensi solo per fare alcuni esempi all'IA, al *Cloud*, alla *Blockchain*, alla robotica, all'IOT, all'ingegneria genetica ed alla neuro-tecnologia, ai veicoli a guida autonoma) ed in grado di modificare e trasformare radicalmente il modo nel quale viviamo, comunichiamo, lavoriamo. A tale rivoluzione si accompagna il termine Industria 4.0, ispirato a un progetto del governo tedesco, introdotto per la prima volta come concetto durante la Fiera di Hannover nel 2011. Tutte le rivoluzioni industriali susseguitesi nel tempo sono state veicolate dalle c.d. "Tecnologie Abilitanti" ovvero tecnologie che hanno avuto un forte impatto non solo sulla produzione ma anche sull'economia e sulla società. Nel XVIII secolo l'invenzione della macchina a vapore ha portato alla prima rivoluzione industriale spingendo da un lato il passaggio da una tipologia di produzione manuale a una prima meccanizzazione della produzione stessa e dall'altro alla urbanizzazione delle persone. La seconda rivoluzione industriale, collocata tra la metà dell'800 ed i primi del '900, ha visto la scoperta dell'elettricità e l'uso del petrolio che hanno portato con l'introduzione della catena di montaggio in ambito industriale alla produzione di massa. La terza rivoluzione industriale, detta anche Rivoluzione Digitale, ha avuto inizio negli anni sessanta e si è diffusa grazie all'introduzione nelle realtà produttive dell'*Information Technology* di prima generazione, ovvero microelettronica, transistor, circuiti integrati, semi-conduttori, microprocessori, Personal Computer, fino all'avvento e successiva diffusione di Internet negli anni novanta. Tutto ciò ha consentito una progressiva automazione della produzione e ha inciso profondamente sui settori bancario, dell'energia e delle telecomunicazioni. La quarta rivoluzione industriale, che stiamo vivendo oggi, è caratterizzata dall'"egemonia del dato", dall'uso estensivo in ambito industriale delle tecnologie digitali e rappresenta una nuova rivoluzione non solo rispetto al modo di produrre e organizzare il lavoro (caratterizzato da una stretta sinergia tra manifattura e servizi), ma anche da una progressiva riorganizzazione della società (si pensi per esempio ai progetti di smart city). Tale rivoluzione porta con sé numerose sfide, opportunità e rischi e un fortissimo impatto su governi, aziende, società civile e singoli individui. Per un approfondimento si veda in particolare: K. Schwab, *La quarta rivoluzione industriale*, Franco Angeli, 2016; Id., *Governare la quarta rivoluzione*, Franco Angeli, 2019; Id., *The Fourth Industrial Revolution: what it means, how to respond*, 2016.

[5]L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017; M. Durante, *Il potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Sesto San Giovanni, 2019.

[6]M. Castells, *The information age. Economy, society and culture*: Volume I, *The rise of the network society* (1996); Volume II, *The power of identity* (1997); Volume III: *End of millennium* (1998). I tre volumi sono stati tradotti in italiano dalla Università Bocconi Editore con i titoli di *La nascita della società in rete* (2002); *Il potere delle identità* (2003); *Volgere di Millennio* (2003); Id., *Identity in the network society. Conversation with Manuel Castells*.

[7]Già nel 1978 Simon Nora e Alain Minc, nel rapporto *Convivere con il calcatore* (Bompiani, 1984), avevano intuito l'essenza rivoluzionaria della telematica come chiave di volta del mondo contemporaneo, in grado di sovvertire i tradizionali rapporti di forza che governano la società. La loro visione di un insieme di strutture telematiche le cui interconnessioni danno vita a nuovi organismi, che assumono caratteristiche sempre più reticolari, ha trovato conferma negli anni Ottanta col dilagare di Internet e del World Wide Web che si configurava da un lato come un potentissimo mezzo di comunicazione, dall'altro come uno straordinario serbatoio di informazioni e di conoscenza. È in tale contesto che maturarono le riflessioni del sociologo Manuel Castells sui legami tra questa forma tecnologica e la pluralità di fenomeni che hanno luogo nel mondo contemporaneo. Nella sua monumentale trilogia, Castells introdusse la nozione di "Informazionalismo", per denotare l'odierna dimensione socio-economica post-industriale. Egli giunse così a definire una "nuova società informazionale", dominata da specifiche forme di organizzazione sociale, in cui la generazione, il trattamento e la trasmissione dell'informazione diventano le risorse fondamentali della produttività e del sapere. Cfr. M. Castells, *op. cit.*

[8]Y. Benkler, *The Wealth of Networks. How social Production Transforms Markets and Freedom*, Yale, 2006.

[9]A livello globale ad ottobre 2020 su una popolazione di 7,81 miliardi erano presenti 5,20 miliardi di smartphone, il 67% della popolazione mondiale possiede un dispositivo mobile. Su 4,66 miliardi di utenti internet (il 60% della popolazione mondiale) 4,14 miliardi sono attivi sui social network, con un tasso di crescita nell'ultimo anno del 12%. Cfr. S. Kemp, *Social media users pass the 4 billion mark as global adoption soars*, in "We are social", October 2020. Su scala nazionale, invece, su una popolazione di 60,51 milioni, il 94% possiede un dispositivo mobile e 49,48 milioni (l'82% della popolazione) ha un accesso ad Internet, mentre 35 milioni di italiani sono attivi sui social, con un tasso di crescita del 6,4%. Cfr. *Digital 2020*, in "We are social", report 2020. Per quanto concerne il consumo di informazioni, secondo uno studio di *Digital news report* solo in Italia i social media coprono il 50% del fabbisogno di notizie degli internauti, mentre la carta stampata prosegue la sua discesa attestandosi intono al 25%. Cfr. *Digital news report*, 2020.

[10]L. Floridi, *The good web – some challenges and strategies to realise it*, in "WWW '18: Proceedings of the 2018 World Wide Web Conference" (Lyon, 23-27 April 2018).

[11]T. Berners-Lee, *Longer biography*.

[12]AGCOM definisce gli OTT «imprese prive di una propria infrastruttura e che in tal senso agiscono al di sopra delle reti, da cui Over-The-Top» e che «forniscono, attraverso le reti IP, servizi, contenuti e applicazioni (...) e traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi agli utenti finali (...) e di spazi pubblicitari». Cfr. AGCOM, *Relazione Annuale 2012 sull'attività svolta e sui programmi di lavoro*, p. 28.

[13]Per un approfondimento sul tema consultare A. Venanzoni, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in "MediaLaws", 2020, n. 3; J. Kotkin, *The Coming of Neo feudalism - a warning to the global middle class*, New York, 2020; P. Grossi, *Unità giuridica europea: un Medioevo prossimo futuro?*, in "Quaderni fiorentini per la storia del pensiero giuridico moderno", 2002, n. 31, pp. 39-57; E. Morozov, *Silicon Valley. I signori del Silicio*, Codice, 2016.

[14]Come ha affermato in modo calzante Andrew Lewis *Se non state pagando qualcosa, non siete un cliente, siete il prodotto che stanno vendendo* in "MetaFilter Community weblog", 2002.

[15]La auto-regolazione, interna alla architettura della rete, basata sul principio di democrazia partecipativa, con il tempo, ha visto una istituzionalizzazione degli incontri, dei summit e dei forum che punteggiano lo spazio digitale, come il *World Summit on the Information Society*. Tutto ciò pone un paradosso: quello di Internet espressione al tempo stesso della più alta progettualità umana e spazio entro cui la regolazione giuridica, a detta di molti, non dovrebbe entrare. Secondo

Pizzetti tale paradosso non fa altro che riproporre uno dei dualismi più arcaici del diritto: il contrasto tra *Physei* e *nomos*. F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

[16]A. Venanzoni, *op. cit.*

[17]L. Lessig, *Code 2.0*, New York, 2006.

[18]F. Galgano, *Lex mercatoria*, Il Mulino, 2001.

[19]S. Rodotà, *La rivoluzione dei diritti da Malala al Datagate*, in "La Repubblica", 15 luglio 2013.

[20]G. Gardini, *Le regole dell'informazione. L'era della post-verità*, Giappichelli, 2017.

[21]European Commission, *The EU Code of conduct on countering illegal hate speech online*.

[22]Si pensi, per esempio alla distinzione tra provider (host, *caching*, *conduit*...) che appare insufficiente a categorizzare le nuove realtà (*cloud service*, *content*, *delivery networks*, *domain name services*), che rendono difficile alle aziende nascenti comprendere a quali norme conformarsi.

[23]Per un approfondimento si veda G. Formici, *Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione europea a Stati terzi, le Conclusioni dell'Avvocato generale nel caso Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems e una storia che rischia di ripetersi*, in "Media Laws", 2020, n. 1; F. Bignami, *Schrems II: The Right to Privacy and the New Illiberalism*, in "Media Laws", 2020, n. 3; G. Churches, M. Zalnieriute, *A Groundhog Day in Brussels: Schrems II and International Data Transfers*, 2020.

[24]G. Finocchiaro, *Digital Services Act: la ridefinizione della limitata responsabilità del provider e il ruolo dell'anonimato*, in "MediaLaws", 2021; F. Paolucci, *Il digital services act: verso una nuova governance di internet?*, in "Iusinitinere.it", 2020.

[25]Secondo il *Corporate Europe Observatory* il maggior numero di incontri è stato ottenuto proprio da Google, Microsoft, Facebook, preoccupate da una potenziale rivisitazione delle norme antitrust annunciata con il DMA, e da una nuova regolamentazione sulle modalità di gestione dei contenuti on-line che ha l'obbiettivo di fissare i principi per la moderazione degli stessi e per la risoluzione di controversie così come previsto nel DSA. Cfr. Corporate Europe Observatory, *Big Tech brings out the big guns in fight for future of EU tech regulation*, 2020.

[26]Risoluzione del Parlamento europeo A3-0282/93 in G.U. n. C 20/113.

[27]C. Mortati, *Istituzioni di diritto pubblico*, II, Cedam, 1969, p. 972.

[28]G. Sartori, *Opinione pubblica*, in "Enciclopedia del Novecento", 1979; G. Rebuffa, *Opinione pubblica e democrazia*, il Mulino, 2003.

[29]P. Bilancia, *Quale democrazia*, in "Federalismi.it", 2017, n. 1; A. Papa (a cura di), *Comunicazione e nuove tecnologie*, Aracne, 2011.

[30]W. Quattrociocchi, A. Vicini, *Misinformation. Guida alla società dell'informazione e della credulità*, Franco Angeli, 2017.

[31]La bolla dei filtri si caratterizza per tre nuove dinamiche: in primo luogo, in un'epoca in cui le informazioni condivise sono alla base di esperienze condivise (si pensi per esempio ad un canale via cavo dedicato ad uno sport che è seguito da telespettatori che hanno una passione in comune), la bolla, invece, ci divide e ci isola nel mondo che ha costruito su misura per noi; in secondo luogo non siamo noi che selezioniamo l'informazione secondo criteri evidenti come avviene nel mondo analogico (si pensi ad esempio alla ricerca di notizie su giornali che hanno un palese orientamento politico) ma è l'informazione che ci viene proposta attraverso criteri occulti (Google non è così trasparente, non ci dice chi pensa che siamo o perché ci mostra i risultati che vediamo sullo schermo); infine non siamo noi a scegliere di entrare nella bolla, non siamo noi a scegliere il colore delle lenti con le quali guardare ed interpretare ciò che ci circonda, ma ci viene suggerito e in modo strisciante condiziona il modo nel quale percepiamo il mondo. E. Pariser, *Il Filtro*, il Saggiatore, 2012.

[32]Cass Sunstein aveva individuato una importante distinzione, quella tra la sovranità del consumatore nel libero mercato e la sovranità del cittadino in una nazione libera; ma quello che va bene per un consumatore non va bene per un cittadino. Se l'informazione tagliata su misura dei gusti del consumatore può rendere più facili e soddisfacenti le sue scelte di consumo, altrettanto non può dirsi per il cittadino. La sovranità politica ha un diverso fondamento che richiede un dibattito pubblico dove possano entrare in contatto e confrontarsi idee diverse e molto distanti tra di loro e soprattutto lontane dall'idea dominante. C.R. Sunstein, *Republic.com 2.0*, Princeton University Press, 2007, p. 38; G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino, S. Quintarelli (a cura di), "Parole e potere. Libertà di espressione, hate speech e fake news", Egea, 2017.

[33]Dopo settimane in cui il mantra *stop the steal* imperversava sui social media mietendo proseliti, sono state sufficienti poche parole del Presidente uscente Donald Trump, pronunciate durante i raduni politici che hanno preceduto la cerimonia di insediamento del nuovo Presidente, amplificate attraverso i social media, in particolare Twitter, in cui questo incitava a mettere in atto una protesta selvaggia e marciare sul Campidoglio per riprendersi il paese, per causare un vero e proprio attacco al cuore della democrazia culminato in scontri violenti e saccheggi. Donald Trump nei suoi raduni del 19, 27, 30 dicembre 2020 ha incitato i propri sostenitori utilizzando le seguenti parole: «[make a] big protest in D.C. on January 6th. Be there, will be wild!» e «We will never give up; we will never concede, we will stop the steal. We're going to walk down Pennsylvania Avenue, and we're going to the Capitol... We're going to try and give our Republicans, the weak ones... the kind of pride and boldness that they need to take back our country». Le stesse parole sono state rilanciate attraverso Twitter dal Presidente uscente il 1° gennaio 2021. Per un approfondimento cfr. D.Z. Morris, *"We will never concede": How Donald Trump incited an attack on America*, 2021.

[34]P. Lévy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, Feltrinelli, 1996.

[35]Il diritto all'informazione e alla comunicazione pubblica, espressione del nuovo rapporto che si è andato delineando a partire dagli anni Novanta tra poteri pubblici e cittadino dove quest'ultimo è sempre più parte integrante delle amministrazioni e non mero amministrato, ha trovato ancoraggio costituzionale nella "Costituzione materiale" in grado di cogliere le modificazioni intervenute nel sistema giuridico e sociale, in misura maggiore rispetto agli schemi dettati dalla "Costituzione formale". Infatti, non basta l'interpretazione estensiva dell'art. 21 Cost. come libertà di informare, informarsi ed essere informati, per fornire al diritto all'informazione pubblica ed al principio di pubblicità dell'agire dei pubblici poteri una solida base costituzionale, né il richiamo e la combinazione con gli art. 64 Cost. (Pubblicità dei lavori delle Camere), 73 (pubblicazione delle leggi) e 97 (buon andamento ed imparzialità della pubblica amministrazione, precetto che maggiormente sostiene l'importanza della pubblicità dell'agire delle pubbliche amministrazioni, espressione dei principi di trasparenza e imparzialità che debbono guidare l'intero agire degli organi amministrativi). Le basi costituzionali del diritto all'informazione pubblica debbono altresì rintracciarsi nelle disposizioni poste a salvaguardia del principio democratico della repubbli-

ca (art. 1), della garanzia dei diritti della personalità (art. 2) e dell'imparzialità (art. 3) fino a ricomprendere la garanzia dell'associazionismo per fini politici (art. 49). Alla luce di tali riflessioni, allora, la "pretesa" degli amministrati a ricevere informazioni troverà giustificazione nel complesso delle norme costituzionali sulle quali si fonda l'ordinamento democratico. Per un approfondimento si veda: P. Barile, *Diritti dell'uomo e libertà fondamentali*, il Mulino, 1984; P. Marsocci, *Poteri e pubblicità. Per una teoria giuridica della comunicazione istituzionale*, Cedam, 2002; G.U. Rescigno, *Corso di diritto pubblico*, Zanichelli, 2001.

[36] F. Faini, *Social open government: l'utilizzo dei social media nell'amministrazione digitale aperta*, in "Informatica e diritto", 2017, n. 1-2; L. Sartori, *Open government: What Else?*, in "Istituzioni del federalismo", 2013, n. 3-4.

[37] E. Carloni, *L'amministrazione aperta: Regole, strumenti e limiti. Dell'open-government*, Maggioli, 2014.

[38] F. Faini, *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in "Cyberspazio e diritto", 2013 n. 2.

[39] I processi di informatizzazione e l'impiego delle moderne tecnologie dell'informazione che hanno profondamente influenzato l'organizzazione dell'attività amministrativa, le singole procedure, i rapporti con l'utenza ed i servizi a questi offerti, nonché gli interventi normativi volti a disciplinare ed agevolare questo processo, ricadano sotto il concetto di *e-government*. Per *e-government* si intende, quindi, quel processo complessivo di ammodernamento dell'amministrazione pubblica, sia sotto il profilo tecnico che giuridico, realizzato grazie all'introduzione e all'applicazione delle nuove tecnologie ICT a tutti gli aspetti strutturali e funzionali dell'amministrazione stessa.

[40] Gli atti di *soft law* hanno il compito di disegnare le politiche di riferimento ed orientare la successiva disciplina giuridica del fenomeno di rango legislativo, la quale ha a sua volta il compito individuare i principi generali e la disciplina specifica di riferimento.

[41] Per un approfondimento si veda G. Arena, *La funzione di comunicazione nelle pubbliche amministrazioni*, Maggioli, 2004; B.G. Mattarella, *Informazione e comunicazione amministrativa*, in "Rivista trimestrale di diritto Pubblico", 2005, n. 1.

[42] Art. 2 c. 2 l. 150/2000 «Le attività di informazione e di comunicazione sono attuate con ogni mezzo di trasmissione idoneo ad assicurare la necessaria diffusione di messaggi, anche attraverso la strumentazione grafico-editoriale, le strutture informatiche, le funzioni di sportello, le reti civiche, le iniziative di comunicazione integrata e i sistemi telematici multimediali».

[43] *Linee Guida per i siti web della PA*, 2011: Art. 6.3 Partecipazione web 2.0 «Il coinvolgimento dei cittadini per migliorare la gestione e la qualità dei servizi offerti dalla pubblica amministrazione ha come precondizione, l'adozione dell'approccio web 2.0 per la comunicazione e condivisione delle risorse online. I social media possono essere considerati dalla pubblica amministrazione come canali di broadcasting ad alto potenziale di audience, dalla forma semplice e di versatile diffusione tra i cittadini, estremamente economici (sia per gli utenti che Amministrazioni pubbliche stesse), multipiattaforma e spesso interoperabili tra loro. Attraverso la pubblicazione in tempo reale di piccoli messaggi di testo (microblogging), immagini, audio e video, si può garantire un'informazione costante e aggiornata, comunicare ed erogare servizi mirati a particolari fasce d'utenza, accrescere la percezione di vicinanza dell'amministrazione ai cittadini. Sono molti gli strumenti utili a questo scopo che in questo momento il web mette a disposizione: forum, wiki, blog, social network, XML e RSS, podcast, georeferenziazione (cfr. per le definizioni la Tabella B.2 nel Vademecum 2010 "Indicazioni operative per la costruzione, lo sviluppo e la gestione dei siti web delle PA"). La strategia d'uso degli strumenti del web 2.0, all'interno della comunicazione web delle amministrazioni, deve tenere conto: del target di riferimento e quindi del ruolo dell'utenza nella costruzione della conoscenza; del contesto organizzativo e dei modelli architetturali in cui verrà implementata. Nella riprogettazione dei servizi e dei contenuti web in una logica 2.0, si raccomanda quindi di: definire l'organizzazione dei contenuti sulla base dei bisogni degli utenti; erogare i servizi secondo una logica multicanale e multi dispositivo; facilitare l'accesso ai dati e alle informazioni attraverso funzionalità evolute di ricerca e localizzazione».

[44] Art. 8.2 *Circolare n. 2/2017*: «Per accrescere la fruibilità delle informazioni di interesse generale e l'efficienza nella gestione delle domande, si raccomanda alle amministrazioni di valorizzare la possibilità di pubblicare informazioni anche diverse da quelle oggetto di pubblicazione obbligatoria, fermo restando il rispetto delle esclusioni e dei limiti previsti dall'art. 5-bis, c. 1-3, del d.lgs. n. 33/2013. In particolare, la pubblicazione proattiva sui siti istituzionali delle amministrazioni è fortemente auspicabile quando si tratti di informazioni di interesse generale o che siano oggetto di richieste ricorrenti: ad esempio, quando si tratti di dati o documenti richiesti, nell'arco di un anno, più di tre volte da soggetti diversi. Per gli stessi motivi, le pubbliche amministrazioni sono invitate a valorizzare il dialogo con le comunità di utenti dei social media (Facebook, Twitter, ecc.). I richiedenti spesso rendono pubbliche su questi mezzi di comunicazione le domande di accesso generalizzato da essi presentate. In questi casi, e comunque quando si tratti di informazioni di interesse generale, è opportuno che anche le amministrazioni utilizzino i medesimi canali a fini di comunicazione».

[45] B. Pang, L. Lee, *Opinion mining and sentiment analysis*, in "Foundations and Trends in Information Retrieval", 2008, n. 1-2.

[46] F. Cardarelli, *Amministrazione digitale, trasparenze e principio di legalità*, in "Il Diritto dell'Informazione e dell'Informatica", 2015, n. 2: «Il diritto all'uso delle tecnologie è qualificabile come una posizione giuridica soggettiva strumentale verso la Pubblica amministrazione, accostabile al paradigma dell'interesse legittimo».

[47] *Vademecum* curato da Formez realizzato nell'ambito delle attività finalizzate alla elaborazione delle Linee guida per i siti web delle Pubbliche Amministrazioni (previste dalla Direttiva n. 8 del 26 novembre 2009 del Ministro per la pubblica amministrazione l'innovazione).

[48] S. Talamo, F. Di Costanzo, R. Crudele (a cura di), *Social Media e PA, dalla formazione ai consigli per l'uso*, Formez PA, 2018.

[49] M. Pietrangelo, *La lingua della comunicazione al tempo di Internet. Profili giuridici*, Esi, 2016.

[50] Per un approfondimento sulla crisi dell'informazione professionale si veda C. Pinelli, *"Postverità", verità e libertà di manifestazione del pensiero*, in "MediaLaws", 2017, n. 1; M. Cuniberti, *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in "MediaLaws", 2017, n. 1.

[51] A. Lovari, *Networked citizens. Comunicazione pubblica e amministrazioni digitali*, Franco Angeli, 2013; I. Mergel, S.I. Bretschneider, *A Three-Stage Adoption Process for social Media Use in Government*, in "Public Administration Review", 2013, n. 3; G. Ducci, *Relazionalità consapevole. La comunicazione pubblica nella società connessa*, Franco Angeli, 2017.

[52] Sul fondamento costituzionale della tipicità degli atti amministrativi si veda E. Ferrari, *Nozione e fondamento costituzionale della tipicità degli atti amministrativi*, in "Rivista AIC", 2019, n. 2.

[53]G. Sgueo, *L'amministrazione digitale*, in "Giornale di diritto amministrativo", 2016, n. 1.

[54]Consiglio di Stato, Sez. VI, 12 febbraio 2015, n. 769; Tar Liguria, sentenza n.787 del 19 maggio 2014. Conformi anche Consiglio di Stato, Sez. V, 24 settembre 2003, n.5444; Cass., Sez. II, 30 maggio 2002, n. 7913; Sez III, 12 febbraio 2002, n. 1970. Per approfondimenti E. Bassoli, *Valenza giuridica del tweet di un ministro*, in "Sicurezza e Giustizia", 2015.

[55]G. Sgueo, *La comunicazione di un Ministro attraverso un social network integra gli estremi di un atto amministrativo?*, in "Giornale di diritto amministrativo", 2015, n. 4; S. Rossa, E. Celeste, *A colpi di tweet: social network, pubblica amministrazione e politica*, in "Istituzioni del federalismo", 2020, n. 1; E. Celeste, *Social media and politics: the legal value of tweet*, in "MediaLaws", 2020, n. 1.

[56]Il ruolo legato alla gestione dei Social Media è il Social Media Manager, figura emersa già nel mondo professionale privato ma ancora in fase di definizione nel settore pubblico. Con il termine *Social Media manager* si intende una persona incaricata di curare e pubblicare i contenuti sui canali Social gestiti da un'organizzazione, elaborando un piano editoriale e interagendo con la community di cui ne rappresenta l'anima. E. Zaccone, *Social Media monitoring*, Flaccovio Editore, 2015.

[57]F. Faccioli, *Comunicazione pubblica e media digitali: la prospettiva del public engagement*, in "Problemi dell'informazione", 2016, n. 1.

[58]A. Lovari, *Social media e pubblica amministrazione tra diritti e doveri: una prospettiva sociologica*, in "Rivista Italiana di Informatica e diritto", 2019, n. 1.

[59]F. Contini, G.F. Lanzara, *ICT and Innovation in the Public Sector. European studies in the framework of e-government*, Palgrave Macmillan, 2009.

[60]M. Weber, *The Theory of social and economic organization*, Collier Macmillan Publisher, 1974.

[61]Controversa e dibattuta la questione sulla natura di servizio pubblico o funzione amministrativa della comunicazione pubblica. La distinzione tra servizio pubblico e funzioni pubblica non ha, infatti, confini netti soprattutto perché anche la fruizione di servizi pubblici implica o può implicare l'esercizio di funzioni autoritative o certificative, ovvero di attività giuridiche culminanti in provvedimenti amministrativi. Per un approfondimento: M.S. Giannini, *Il pubblico potere. Stati e amministrazioni pubbliche*, il Mulino, 1986; F. Merloni, *Istituzioni di diritto amministrativo*, Giappichelli, 2012; G. Cammarota, *I servizi pubblici on-line*, in G. Cammarota, P. Zuddas (a cura di), "Amministrazione elettronica: caratteri finalità e limiti", Giappichelli, 2020; M. D'Alberti, *Lezioni di diritto amministrativo*, Giappichelli, 2019; G. Corso, *Manuale di diritto amministrativo*, Giappichelli, 2008.

[62]E. Franceschini, *Azioni in calo, ecco perché Twitter ha riammesso Trump*, in "la Repubblica", 8 gennaio 2021.

[63]Twitter, *Permanent suspension of @realDonaldTrump*, Jan. 8, 2021.

[64]La definizione di "comunicazione pubblica" che ad oggi appare più completa, ricomprendendovi sia la dimensione oggettiva che soggettiva, è quella data da Franca Faccioli la quale, senza pretese di esaustività, definisce l'ambito della comunicazione pubblica come "processo complesso al quale partecipano soggetti con ruoli e responsabilità diversi, che agiscono nell'ambito dello stesso contesto e nella prospettiva di contribuire alla realizzazione dell'interesse della collettività ... essa fa interagire attori pubblici e privati nella prospettiva di attivare la relazione tra Stato e cittadini ... suo oggetto sono temi di interesse generale e sua finalità è contribuire alla realizzazione di tale interesse"; cfr. F. Faccioli, *Comunicazione pubblica e cultura del servizio*, Carocci editore, 2008. La "comunicazione istituzionale" è "la spina dorsale dell'intero sistema della comunicazione pubblica" ed è possibile definirla come quella comunicazione promossa da una pubblica amministrazione (o ente pubblico o servizio pubblico) sia centrale che periferica e la cui fonte è riconosciuta come tale da tutti i destinatari del messaggio per mezzo di segni distintivi espliciti e chiari. Pubblicizza la produzione normativa, le attività, le funzioni, l'identità e il punto di vista dell'amministrazione attraverso l'utilizzo, in maniera integrata, di tutti i media a disposizione (stampa, radiotelevisione, la rete) avvalendosi dei diversi registri comunicativi di questi mezzi. Si rivolge ai cittadini ed ai gruppi dell'ambiente sociale in cui svolge la sua attività (comunicazione esterna diretta); ai mass media (quando tramite il medium vuole raggiungere cittadini e organizzazioni); a chi opera all'interno delle istituzioni pubbliche (comunicazione interna). Scopo principale è quello di assicurare ai cittadini una completa informazione sulle realtà delle organizzazioni pubbliche e sulle norme vigenti (espressione del diritto di informarsi e di essere informati), nonché costruire e promuovere l'identità dell'ente pubblico al fine di valorizzare l'immagine dell'istituzione e rafforzare i rapporti tra l'istituzione e i cittadini anche in termini di legittimazione dell'istituzione stessa. La comunicazione è sempre più una risorsa strategica per stabilire con i cittadini un rapporto relazionale basato sull'ascolto e tendente alla realizzazione di un modello di "amministrazione condivisa" con i cittadini, non più meri amministrati ma soggetti attivi e co-amministratori; cfr. G. Arena, *La funzione di comunicazione nelle pubbliche amministrazioni*, Maggioli, 2004. La "comunicazione politica", invece, interviene su argomenti di interesse generale aventi carattere controverso e rispetto ai quali sostiene un particolare punto di vista. Gli attori in gioco sono il sistema politica, il sistema dei *mass media* e il cittadino-elettore. Questo tipo di comunicazione si sostanzia nel dibattito politico ovvero nella esposizione delle idee e delle linee strategiche delle forze politiche e nella gestione delle campagne elettorali. Scopo è quello di costruire, mantenere, rafforzare il consenso. Determinanti in questo tipo di comunicazione sono i media di massa (prima la radiotelevisione ed oggi sempre di più internet ed i *social network*) che sfruttano le tecniche di persuasione del *marketing* e della pubblicità per veicolare il proprio messaggio, esprimere senso di vicinanza al popolo, promuovere le immagini dei singoli candidati o dei partiti politici, in una parola fare propaganda; cfr. P. Marsocci, *op. cit.*, pp. 182 ss. La "comunicazione sociale", infine, ha quale scopo quello di sensibilizzazione l'opinione pubblica su temi di interesse collettivo. L'istituzione pubblica nell'attivare una campagna di comunicazione sociale sarà sempre guidata da un fondamento normativo, sia quando prevista da una legge nazionale sia quando questa attività sia rimessa alla propria discrezionalità (si pensi ad es. alla tutela dell'ambiente, della salute, ordine pubblico). In particolare gli obiettivi principali della comunicazione sociale sono: Informare e aggiornare, ossia portare all'attenzione del pubblico un concetto positivo, un progetto sociale, un intervento da condividere, un'azione responsabile, un'innovazione tecnologica; convincere e persuadere, cioè presentare e "argomentare" attraverso dati, ricerche, testimonianze utili a dimostrare la veridicità di quanto comunicato; infine stimolare e motivare e, quindi, proporre nuovi modelli di comportamento, stimolare azioni destinate a contribuire ad una causa sociale, modificare concezioni errate; cfr. G. Gadotti, *La comunicazione sociale, soggetti, strumenti e linguaggi*, Arcipelago edizioni, 2001, p. 207; R. Grandi, *La comunicazione pubblica: teorie, casi, profili normativi*, Carocci, 2007.

[65]G. Arena, *La funzione di comunicazione nelle pubbliche amministrazioni*, Maggioli, 2004. Arena, per esempio, distingue tre diversi tipi di comunicazione istituzionale: la "comunicazione giuridico-formale": volta ad applicare norme, fornire certezze ottenere la conoscibilità giuridica di un atto e altre simili attività (es. certificazioni, verbalizzazioni, no-

tificazioni, pubblicazioni su fogli ufficiali, raccolte ufficiali di atti, affissioni ad albi, registri etc.); la "comunicazione di servizio": diretta ad informare gli utenti sulle modalità di funzionamento degli uffici , sulla normativa applicata, le prestazioni offerte". Si tratta di informazioni che di per sé costituiscono già un servizio agli utenti e sono contemporaneamente parte integrante del servizio offerto dall'amministrazione; la "comunicazione amministrativa o comunicazione di cittadinanza": è la più significativa ai fini della realizzazione della amministrazione condivisa, non serve per regolare i rapporti giuridici o per informare circa un fatto della vita quotidiana ma per risolvere un problema di interesse generale (es. tutela ambientale, sanità, previdenza, etc.).

[66]A tale proposito anche il Garante per la Privacy, a seguito del d.lgs. 33/2013 in materia di pubblicità e trasparenza delle pubbliche amministrazioni ed obblighi di pubblicazione sul web previsti dalle disposizioni di riferimento, è intervenuto dettando le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"; cfr. Garante per la protezione dei dati personali, *La trasparenza sui siti web della PA. Le linee guida per il trattamento dei dati personali*, 2014. In particolare, tali Linee Guida hanno introdotto una serie di disposizioni per armonizzare il quadro regolamentare e hanno indicato modalità e accorgimenti che i soggetti pubblici sono tenuti ad applicare quando "diffondono" dati personali sui propri siti web istituzionali per finalità di trasparenza o per garantire altri obblighi di pubblicità degli atti amministrativi. È necessario distinguere le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza da quelle che regolano forme di pubblicità per finalità diverse (es.: pubblicità legale, pubblicità integrativa dell'efficacia, pubblicità dichiarativa o notizia). Il d.lgs. 33/2013 definisce "pubblicazione" l'inserimento nei siti istituzionali delle P.A. di documenti, informazioni e dati "concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" (art. 2, comma 2); da ciò si deduce che tutte le volte in cui nel decreto è utilizzata la locuzione "pubblicazione obbligatoria ai sensi della normativa vigente" il riferimento è limitato alla pubblicazione che concerne l'organizzazione e l'attività delle P.A. Per tale motivo, tutte le ipotesi di pubblicità "non" riconducibili a finalità di trasparenza, qualora comportino una diffusione di dati personali, sono escluse dall'applicazione del d.lgs. 33/2013. Con il Regolamento (UE) 2016/679 (c.d. GDPR) assistiamo ad un mutamento del quadro normativo in materia di pubblicità della PA. Le disposizioni contenute nel GDPR sono direttamente applicabili e non possono essere derogate dalla disciplina nazionale in virtù del primato del diritto europeo: da tale principio discende l'obbligo di interpretare il diritto nazionale in maniera conforme al diritto europeo. Quindi anche la pubblicazione di dati personali è soggetta al rispetto dei principi del GDPR (art. 5) ed è consentita soltanto quando ricorre una delle condizioni di cui all'art. 6 che rendono lecito il trattamento (consenso, contratto, obbligo di legge, interesse vitale, interesse pubblico, legittimo interesse). L'art. 4, n. 1, GDPR intende per "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Il legislatore europeo, inoltre, prestando particolare attenzione al trattamento di categorie particolari di dati personali (prima erano c.d. dati sensibili), all'art. 9, par. 1, GDPR stabilisce che «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Al par. 2, relativamente alla casistica che ci occupa, tale divieto non si applica se si verifica che «g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

[67]F. Faccioli, *Comunicazione pubblica e cultura del servizio*, cit.

[68]Si ricordino inoltre, le prime avanzate esperienze di informatizzazione della normativa, avviate in Italia negli anni '70, come l'implementazione del progetto "Norme in rete" e del CED (Centro di documentazione elettronico della Corte di Cassazione). Per un approfondimento: M. Pietrangelo, *La conoscibilità della legge per via informatica e telematica*, in "Informatica e diritto", 2006, n. 2, pp. 245-272; P. Costanzo, *La pubblicazione normativa al tempo di internet*, in AA.VV., "Le fonti del diritto, oggi. Giornate di studio in onore di Alessandro Pizzorusso", Edizioni Plus, 2006. E. Albanesi, *Il principio della gratuità della fruizione della Gazzetta ufficiale telematica*, in "Il diritto dell'informazione e dell'informatica", 2012, n. 3, p. 481 ss.

[69]A titolo esemplificativo nei siti del Quirinale, del Senato, della Camera dei Deputati sono rinvenibili apposite sezioni dedicate ai Provvedimenti, agli Atti adottati o collegamenti a pagine di altri canali dedicati alle loro attività. In particolare si veda nel sito della Presidenza del Consiglio dei Ministri la sezione dedicata a Normattiva: il portale della legge vigente, ma anche il sito della Gazzetta Ufficiale della Repubblica Italiana ed i portali Regionali dove è possibile rinvenire apposite sezioni volte a diffondere la conoscenza di leggi, regolamenti e atti regionali (si pensi al BURT: Bollettino Ufficiale della Regione Toscana che dal gennaio 2008 esce solo in versione telematica). È bene precisare però che l'unico testo definitivo è quello pubblicato sulla Gazzetta Ufficiale a mezzo stampa che prevale in caso di discordanza.

[70]R. Grandi, *op. cit.*; P. Marsocci, *op. cit.*

[71]Ormai diventati famosi i Tweet dell'ex Presidente Trump contenenti spesso attacchi personali e diretti ad altri esponenti politici o del suo staff fino alle bagarre con il dittatore coreano Kim Jong-un.

[72]Una delle poche soluzioni che permettono di studiare i sentimenti di un testo anche in lingua italiana è quella di Syuzhet Package. Quest'ultimo utilizza il linguaggio di programmazione R e Phyton. Per un approfondimento cfr. A. Aversano, *L'analisi di Twitter tramite il software R. Breve guida pratica. Seconda parte*, 2020; M. Jockers, *Introduction to the Syuzhet Package*, 2020.

[73]In particolare, l'art. 9 della L. 28/2000 stabilisce che «Dalla data di convocazione dei comizi elettorali e fino alla chiusura delle operazioni di voto è fatto divieto a tutte le amministrazioni pubbliche di svolgere attività di comunicazione ad eccezione di quelle effettuate in forma impersonale ed indispensabili per l'efficace assolvimento delle proprie funzioni». Gardini fa notare che la ratio della norma è anzitutto evitare che l'attività di comunicazione istituzionale realizzata dall'amministrazione durante questo periodo "sensibile" possa sovrapporsi con l'attività propagandistica svolta dalle liste e dai candidati, dando vita ad una forma parallela di campagna elettorale, sottratta a qualsiasi tipo di regolamentazione. In secondo luogo, la norma vuole impedire il consolidarsi di un vantaggio elettorale a favore dei politici uscenti (*incumbents*)

nei confronti degli sfidanti (*challengers*), date le innumerevoli facilitazioni, in termini di comunicazione e di visibilità, di cui i primi dispongono in via esclusiva e gratuita. Da ultimo, ma non in ordine di importanza, la norma mira ad evitare un uso distorto di risorse e denaro pubblico a fini di propaganda (diretta o indiretta) favorevole ad alcune forze politiche e a danno di altre. Tuttavia, tale legge sembra essere costantemente disattesa dalle operazioni di comunicazione proprio sui social media e non in grado di arginare la costante commistione tra comunicazione delle attività istituzionali e politica. Cfr. G. Gardini, *Brevi note sul divieto di comunicazione istituzionale nei periodi di campagna elettorale*, in "MediaLaws", 2018, n. 3.

[74]Vedi le Campagne di pubblicità progresso.

[75]E. Invernizzi, *Manuale di Relazioni Pubbliche 2. Le competenze e i servizi specializzati*, McGraw-Hill, 2006. Invernizzi definisce la comunicazione interna come «l'insieme delle attività specialistiche di comunicazione necessarie a supportare il funzionamento, lo sviluppo e il successo delle organizzazioni complesse. Tali attività che devono essere gestite ed integrate tra di loro con un'adeguata attività manageriale, possono essere suddivise in quattro categorie, ciascuna con uno specifico obiettivo. La comunicazione strategica, per indirizzare e coinvolgere le persone dell'organizzazione. La comunicazione creativa, per generare le conoscenze e le competenze necessarie. La comunicazione della conoscenza o formativa, per diffondere le competenze distintive dell'organizzazione. La comunicazione funzionale, per supportare i processi gestionali e produttivi».

[76]Vedi Urp degli Urp. Comunicazione pubblica in rete.

[77]Per quanto concerne il flusso di dati al di fuori dell'Ue trova una propria disciplina agli art. 44, 45, 46,47,48,49,50 contenuti nel Capo V del GDPR dedicato al "Trasferimento di dati personali verso paesi terzi ed organizzazioni internazionali". L'art. 44 prevede che «qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato». All'art. 45 c. 1 si prevede che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. Nei commi successivi si elencano le condizioni richieste affinché si consideri un livello di protezione come adeguato. In assenza di decisioni di adeguatezza della Commissione sono richieste garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa – BCR e clausole contrattuali modello) (art. 46 GDPR); in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (art. 49 GDPR). Alle autorità europee sarà, quindi, richiesto in assenza di decisioni di adeguatezza della Commissione europea (come nel caso del *Privacy Shield* Ue-Us che come abbiamo visto è stato invalidato dalla sentenza *Sherms II* proprio perché non in grado di offrire le stesse garanzie ai cittadini europei nel trattamento dei loro dati) di effettuare valutazioni d'impatto sul trasferimento dei dati caso per caso, per identificare se nel paese terzo di destinazione è garantito un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione (*Transfert Impact Assessment*). Qualora dall'*assessment* emerga che non sia possibile assicurare, nel paese in cui si intende trasferire i dati, un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione, le autorità, insieme ai *data importers* dovranno identificare le misure supplementari da mettere in atto, sfruttando i documenti elaborati nella prima fase (mappature e relative valutazioni). In base all'esito delle mappature unitamente alle valutazioni di impatto l'EDPS (Garante europeo per la protezione dei dati) stabilirà in cooperazione con EDPB (Comitato europeo per la protezione dei dati) le priorità a lungo termine per garantire la conformità al GDPR per il futuro.

[78]Cfr. AgID, *Contenuti e linguaggio. Usa il linguaggio giusto per i tuoi utenti e organizza i contenuti del tuo progetto digitale*; si veda inoltre M. Pietrangelo, *Il linguaggio giuridico-istituzionale sul web e la disinformazione pubblica on-line*, in "Federalismi.it", 2020, n. 11.

[79]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.

[80]*Il Signore delle Mosche* è un romanzo del 1954 dello scrittore inglese William Golding. Il libro ha come protagonisti un gruppo di ragazzi britannici bloccati su un'isola disabitata e racconta il loro disastroso tentativo di autogovernarsi. Ben presto qualcosa comincia a non funzionare come dovrebbe, emergono difatti paure ancestrali del tutto irrazionali e comportamenti antisociali, da cui si sviluppa una vicenda che metterà a nudo gli aspetti più selvaggi e bestiali della natura umana.

[81]E ciò emerge in modo chiaro dalle parole di Zuckerberg in uno scambio di mail con il CFO David Ebersman rivelate durante una udienza dell'Antitrust americana nel luglio del 2020: «There are network effects around social products and a finite number of different social mechanics to invent. Once someone wins at a specific mechanic, it's difficult for others to supplant them without doing something different». Con questa affermazione Zuckerberg sostiene che è possibile attrarre e fidelizzare una vasta platea di utenti attraverso l'utilizzo di argomenti o specifiche modalità di interazione social. In particolare in questo passaggio il CEO di Facebook sembra preoccuparsi della tendenza degli utenti a prediligere social dedicati a temi specifici e che offrono modelli di interazione innovativi e della difficoltà dei social generalisti come Facebook di riguadagnare l'attenzione di questi utenti una volta persa. C. Newton, N. Patel, *'Instagram can hurt us': Mark Zuckerberg emails outline plan to neutralize competitors*, in "The Verge", 2020. In tal senso si pronunciano anche i direttori regionali di We are social i quali sostengono che il mercato dei social media si sta sempre più spostando da un paradigma generalista ad uno particolarista, favorendo piattaforme che trattano argomenti di nicchia legati ad aspetti specifici dello stile di vita degli utenti; Cfr. S. Varaldo, *We are social trends 2021. Part 2*, 2021.

[82]Sulle numerose funzionalità di *Slack* si veda il sito stesso alla pagina *Una piattaforma per il tuo team e il tuo lavoro*.

[83]Per maggiori dettagli sulle tipologie di *cloud computing* si veda AWS, *Tipi di Cloud computing*.

[84]Si veda *Io.it - l'applicazione dei servizi pubblici*.

[85]Cfr. il *Catalogo dei servizi cloud per la PA qualificati*.

[86]Si vedano rispettivamente le pagine dedicate al *servizio cloud del Friuli Venezia Giulia* e a *quello della Regione Toscana*.

[87]Cfr. *Gaia-X: A Federated Data Infrastructure for Europe*.

[88]Così riferiva il ministro Colao durante il *question time alla Camera dei Deputati il 31/3/2021*.

[89]Cfr. AgID, *Online il nuovo Portale dati.gov.it*, 2021.

On-line public communication and public administration digitalisation between pandemic and infodemic: which prospects for the future?

Abstract: Based on the observation of the new social communication paradigms and their influence on the dialectics of the democratic processes in the current hyperconnected society, the paper aims to probe the opportunities and risks connected to the adoption of the new social media by Public administrations and the role of the institutional communication in their processes of digital transformation. The paper also aims to verify the limits and the adequacy of the technical and legal actions currently put in place, in order to open up a debate on prospects for the future.

Keywords: Public communication – Public administration digitalisation – Infodemic – E-Citizenship – Digital sovereignty – Social media – Cloud – Public opinion – Internet

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0030

Carenze attuali e soluzioni future nei meccanismi per la cooperazione digitale

Laura Abba

La pubblicazione della *Road map for digital cooperation* del Segretario Generale delle Nazioni Unite rappresenta una tappa fondamentale, frutto del lavoro realizzato congiuntamente dalle numerose organizzazioni che operano nell'ecosistema Internet e che da anni sono impegnate in una complessa attività di ridefinizione dei sistemi esistenti in materia di cooperazione digitale. Anche alla luce degli effetti provocati dalla pandemia Covid-19, vengono evidenziate, in termini di criticità, le lacune e le sfide urgenti che si manifestano nell'ambito della governance globale della Rete, per poi definire, in una prospettiva costruttiva e propositiva da realizzare nell'immediato futuro, le azioni necessarie a rafforzare la cooperazione digitale globale proponendo l'opportunità di valorizzare le dinamiche partecipative dell'Internet Governance Forum, all'insegna di una maggiore comunicazione, collaborazione e interazione tra gli *stakeholder*. Rispetto al passato, quando il World Summit on Information Society, WSIS, era l'unico meccanismo intergovernativo che si occupava di questioni politiche pubbliche legate a Internet, oggi esistono, come rilevante inedita novità, diversi meccanismi di negoziazione "para-istituzionali" anche di tipo informale dentro e fuori il sistema delle Nazioni Unite. In tale mutato scenario, prendendo atto della centralità che Internet assume nel panorama internazionale, si rende necessario definire un approccio concreto di sinergica cooperazione internazionale per risolvere in modo efficace le questioni riguardanti la digital governance, superando l'attuale fase di stallo che impedisce la possibilità di rivitalizzare i processi attualmente esistenti.

Connettività globale – Beni pubblici digitali – Inclusioni digitali – Cultura digitale – Diritti umani nell'era digitale – Intelligenza artificiale – Fiducia e sicurezza digitale – Governance digitale

Sommario: *1. Introduzione – 2. Roadmap delle Nazioni Unite sulla cooperazione digitale – 3. Costruire un'architettura più efficace per la governance digitale – 4. Considerazioni conclusive.*

1. Introduzione

Il presente contributo mira ad approfondire le prospettive evolutive della cooperazione digitale[1] configurabile a livello internazionale, alla luce di quanto recentemente tracciato nella *Road map for digital cooperation*[2], report del maggio 2020, diffuso dal Segretario Generale dall'ONU, António Guterres, come ultima ulteriore tappa attuativa del percorso di compartecipazione globale costruito nell'ambito delle svariate iniziative predisposte nel corso del tempo a presidio della gestione coordinata della Rete con l'intento di rafforzare l'approccio inclusivo, trasparente, aperto e paritario (riconducibile al modello *multi-stakeholder*) nella governance di Internet[3], dando continuità progettuale alla visione operativa, risalente ai primi anni del nuovo Millennio, formalizzata in occasione del World Summit on the Information Society (WSIS)[4].

Poiché nell'ultimo decennio le tecnologie hanno determinato cambiamenti radicali per la società nel suo complesso, generando non solo vantaggi ma anche inediti problemi per l'ecosistema digitale, la necessità di migliorare la cooperazione digitale globale

L. Abba è Dirigente tecnologo presso l'Istituto di informatica e telematica del Consiglio Nazionale delle Ricerche (IIT-CNR); è membro del consiglio scientifico della Rivista. Articolo non sottoposto a referaggio.

si manifesta come esigenza prioritaria sia in funzione dello sviluppo efficace dei processi di funzionamento tecnico su cui si fonda l'infrastruttura tecnica di Rete, ma soprattutto per assicurare agli utenti la fruizione generale e consapevole dei benefici offerti dalla Rete in grado di offrire opportunità di crescita economica e di benessere sociale senza precedenti, a condizione che siano predisposti meccanismi co-decisionali uniformi e omogenei finalizzati alla promozione globale della cultura digitale.

In controtendenza rispetto agli attuali sforzi di cooperazione digitale limitati al livello locale, nazionale e regionale[5], l'interdipendenza tecnologica transnazionale richiede di intervenire su scala globale, come sfida urgente estremamente difficile da affrontare per ottenere risultati concreti e tangibili, a maggior ragione in un momento storico in cui, l'emergenza sanitaria "Covid-19" ha ridotto le occasioni di collaborazione disincentivando le relative – sia pure precarie – dinamiche interattive e partecipative.

In tale prospettiva, la Roadmap indica la strada per soddisfare i bisogni emersi con forza negli ultimi anni identificabili secondo le seguenti linee di intervento[6]:

- aggiornare la definizione di Internet Governance dal WSIS Tunis Agenda[7] (2005);
- aiutare i nuovi attori, la politica e le istituzioni a capire la natura e la complessità delle questioni in gioco;
- creare nuovi meccanismi di cooperazione digitale partendo dagli esempi di successo del mondo tecnico della rete[8].

Rispetto alla "storica" istituzione dell'*Internet Governance Forum* (IGF)[9] come peculiare processo partecipativo soggetto a revisione periodica[10], la costante evoluzione della Rete sembra giustificare una profonda ridefinizione dei principi fondanti il governo di Internet, senza però disperdere il consistente patrimonio "valoriale" di esperienze e buone pratiche raccolte. Occorre dunque stimolare una riflessione attenta e particolareggiata sulle attuali criticità esistenti auspicandone il relativo superamento anche in funzione del necessario potenziamento degli assetti da migliorare in una logica sostanziale di fattivo "restyling" dei processi attuali ben oltre la mera apparenza di formali correttivi.

Solo così sarà possibile rivitalizzare lo stato attuale di precaria stabilità dell'ecosistema della Rete progressivamente erosa dal sempre più evidente primato egemonico degli interessi economici di cui sono portatori le grandi multinazionali del settore digitale, al punto da indebolire il "peso" dei governi nazionali e delle organizzazioni internazionali, rendendo altresì pressoché marginale il ruolo decisivo della società civile[11].

Prendendo atto di un progresso evolutivo lento e difficile da realizzare, alla ricerca di un'alternativa concreta configurabile nell'ambito della cooperazione digitale globale, La Roadmap delle Nazioni Unite offre l'opportunità di contrastare i processi centrifughi e di promuovere un "approccio olistico"[12] ispirato ad una visione di Internet come una rete decentralizzata di reti, in grado di collegare tutti e tutto ovunque, nonché aperta alla generale comunità di *stakeholder* interessati[13].

2. Roadmap delle Nazioni Unite sulla cooperazione digitale: sfide, obiettivi e prospettive del futuro digitale a livello globale

La *Roadmap for Digital Cooperation* è il documento pubblicato nel 2020 dalle Nazioni Unite con l'intento di formalizzare una serie di raccomandazioni rivolte alla comunità internazionale per garantire che tutte le persone siano connesse, rispettate e protette nell'era digitale secondo omogenei standard di tutela definiti a livello globale.

Prendendo atto dell'importanza centrale delle tecnologie nel panorama mondiale[14], la Roadmap delinea una visione digitale all'avanguardia da attuare mediante l'implementazione di specifiche azioni in grado di assicurare lo sfruttamento dei benefici offerti dalle ICT, riducendo al minimo i potenziali pericoli in danno degli utenti di fronte a questioni sempre più complesse come l'intelligenza artificiale, la protezione dei dati, la sorveglianza, la privacy, l'ecosistema di Internet, il regime di responsabilità online e la sicurezza che richiedono uno sforzo multilaterale teso a migliorare la cooperazione digitale sotto l'egida delle Nazioni Unite per rendere la relativa governance una priorità globale.

La Roadmap è il risultato di un intenso lavoro a cura dell'High-level Panel on Digital Cooperation (UN-HLPDC)[15] istituito dal Segretario generale delle Nazioni Unite nel luglio 2018[16] per rafforzare la cooperazione sinergica tra le parti interessate che operano nel settore digitale secondo il tradizionale approccio *multi-stakeholder*, sensibilizzando l'opinione pubblica sull'impatto pervasivo delle tecnologie digitali nella società e nell'economia verso un futuro digitale sicuro e inclusivo per tutti a presidio dei diritti umani. In tal senso, Vinton Cerf, uno dei padri di Internet e co-inventore dei protocolli Tcp/Ip, fu da subito entusiasta dell'iniziativa del Segretario Generale dall'ONU, sin dalla denominazione attribuita al

Panel, che non contiene più la parola "Internet" ma "Digital" chiarendo una volta per tutte che il settore digitale è estremamente più ampio del concetto specifico della Rete. Una scelta felice - anche per Fadi Chehadé, Presidente di ICANN[17] dal 2012 al 2016 - che coincide con un momento cruciale di sfiducia da parte dei cittadini, degli operatori tecnologici e della società civile, da cui discende l'esigenza di elaborare nuovi meccanismi di cooperazione[18].

Il citato gruppo di esperti incaricati di elaborare un insieme di linee guida sull'uso ottimizzato delle tecnologie come fattore trainante dell'innovazione in grado di accelerare gli obiettivi di sviluppo sostenibile dell'Agenda 2030, ha pubblicato nel 2019 il rapporto finale *The Age of Digital Interdependence*[19], ove sono individuate cinque raccomandazioni generali[20] funzionali ad affrontare le sfide legate alla trasformazione digitale della società nel suo complesso, che richiedono un deciso cambio di paradigma nella gestione dei processi di innovazione tecnologica per promuovere efficaci condizioni di crescita economica e benessere collettivo:

1. Costruire un'economia e una società digitali inclusive;
2. Sviluppare la capacità umana e istituzionale;
3. Proteggere i diritti umani e la capacità di agire intenzionalmente nel contesto sociale;
4. Promuovere la fiducia digitale, la sicurezza e la stabilità;
5. Promuovere la cooperazione digitale globale.

In particolare, si sollecita la creazione di un ecosistema digitale inclusivo fondato su fiducia, sicurezza e stabilità, ove sia diffusamente disponibile l'accesso universale alla Rete in grado di favorire l'uso consapevole delle tecnologie rispetto al preoccupante scenario di ritardo infrastrutturale e cognitivo che impedisce ad una percentuale significativa della popolazione mondiale la possibilità di fruire dei vantaggi offerte dal digitale in mancanza di adeguati standard di connettività a banda larga ultraveloce nell'ambito di uno scenario ulteriormente aggravato dal persistente deficit di competenze con gravi ricadute sulla tutela dei diritti umani fondamentali esposti a sistemi di sorveglianza da parte di sempre più sofisticati algoritmi[21].

In tale prospettiva, preso atto dell'esigenza di rendere l'Internet Governance Forum più reattivo e pertinente alle problematiche rilevate secondo un modello di architettura decisionale dotata di poteri vincolanti per definire questioni urgenti di politica strategica sul futuro della Rete, garantendo risultati concreti riscontrabili nel perseguimento di tali finalità, viene auspicata la necessità di valorizzare un nuovo modello di cooperazione digitale globale come imprescindibile strumento di dialogo partecipativo che consenta di facilitare la definizione di una visione condivisa a livello internazionale secondo principi, valori e obiettivi da perseguire mediante lo sforzo congiunto di governi, società civile, settore privato e accademico[22].

Sulla base delle raccomandazioni formulate dall'High-level Panel on Digital Cooperation, tenuto conto degli ulteriori contributi pervenuti nel tempo[23], il Segretario generale delle Nazioni Unite, con il supporto dell'*Office of the Envoy on Technology*, ha pubblicato una tabella di marcia per la cooperazione digitale che delinea il percorso con cui la comunità internazionale può sfruttare al meglio le opportunità offerte dalle tecnologie digitali secondo l'individuazione di otto azioni chiave[24].

2.1. La connettività globale

In particolare, come primo obiettivo prioritario il documento sottolinea la rilevanza della "connettività globale" considerata presupposto indispensabile di partecipazione inclusiva nella società digitale. A fronte, infatti, di un teorico 93% di penetrazione complessiva della banda larga mobile, solo il 53,6% della popolazione mondiale usa Internet, mentre circa 3,6 miliardi di persone risultano senza accesso alla Rete, soprattutto nel contesto dei paesi meno sviluppati a reddito medio basso. Tale scenario risulta nondimeno aggravato dalla carenza di competenze digitali minime attestate al 19% del totale con conseguente incremento del divario digitale.

Un ulteriore fattore limitante della copertura tecnologica infrastrutturale è identificabile nell'eccessiva onerosità, in termini di costi, dei sistemi di installazione di connessioni a banda larga. Le condizioni di mercato invero tendono a disincentivare i fornitori ad effettuare investimenti improduttivi e poco profittevoli sul piano del rendimento economico-aziendale rispetto al costo dei servizi offerti agli utenti mediamente superiore al 20% del reddito nazionale lordo mensile pro capite[25].

2.2. I beni pubblici digitali

Superando l'attuale impostazione regolatoria tradizionalmente concepita a protezione rafforzata dei modelli di copyright secondo un approccio proprietaristico privato che ha determinato la rapida concentrazione di poteri monopolistici e oligopolistici con conseguente contrazione delle dinamiche concorrenziali dei mercati, costituisce un'ulteriore azione chiave evidenziata dal Report l'esigenza di qualificare universalmente come "beni pubblici digitali" i software open source, gli Opendata e i modelli di IA con

standard aperti a beneficio di tutta la comunità internazionale. L'obiettivo è favorire il pieno potenziale delle tecnologie così sfruttando equamente la ricchezza del digitale secondo parametri concreti di sviluppo sostenibile conformi ai principi fondanti la nascita di Internet come sistema sperimentale di condivisione delle risorse gestito in modo aperto, inclusivo, sicuro e trasparente.

2.3. L'inclusione digitale

Anche l'esigenza di garantire la "inclusione digitale" rientra tra le finalità di cooperazione internazionale perseguite dalle Nazioni Unite mediante l'elaborazione di efficaci politiche pubbliche da realizzare a fronte di una diffusione disomogenea delle tecnologie che provoca gravi forme di disuguaglianze sociali, culturali ed economiche nell'ambito di un crescente divario digitale esistente soprattutto a discapito dei soggetti più vulnerabili esclusi dalla possibilità di fruire delle tecnologie (migranti, rifugiati, anziani, giovani, persone con disabilità, soggetti residenti in aree rurali) con implicazioni negative di criticità destinate ad aumentare nel corso del tempo al punto da giustificare un maggiore sostegno economico in favore dei paesi in via di sviluppo per recuperare il ritardo riscontrato.

2.4. La cultura digitale

L'inclusione digitale, come rilevante fattore di uguaglianza sociale, si pone in stretta correlazione all'azione chiave definita in materia di "cultura digitale" che mira al potenziamento delle competenze ICT al fine di favorire l'uso consapevole delle tecnologie, garantendo la sicurezza e la protezione degli utenti in grado di acquisire skills professionali aggiornati e conformi alle nuove esigenze del mercato del lavoro ove si prevede nell'imminente futuro la creazione di nuove opportunità occupazionali basate sul possesso di abilità digitali qualificate[26].

2.5. I diritti umani nell'era digitale

Considerando Internet alla stregua di uno spazio sicuro per la condivisione delle informazioni, garantire la protezione dei "diritti umani digitali" rappresenta un'ulteriore complessa sfida globale resa necessaria dall'esigenza di ridurre i pericoli configurabili online a discapito degli utenti esposti – spesso inconsapevolmente – al rischio di censure, manipolazioni e sorveglianze repressive tali da richiedere la generale revisione delle normative vigenti per colmare le lacune legislative sempre più inadeguate a disciplinare lo spazio virtuale della Rete, con particolarmente riferimento alla materia della protezione dei dati personali secondo il rispetto cogente di principi regolatori omogenei affidati al controllo giurisdizionale di autorità indipendenti legittimate ad operare a livello globale anche al fine di contrastare lo strapotere delle grandi imprese multinazionali che operano nel settore "high-tech".

2.6. L'Intelligenza artificiale

Poiché l'intelligenza artificiale, come tecnologia emergente sempre più diffusa, può fornire enormi vantaggi alla società, alle imprese e alle persone, si rendono necessari maggiori sforzi *multi-stakeholder* in sede di cooperazione globale nel settore "IA" per contribuire a implementarne lo sviluppo affidabile, sicuro e sostenibile, prevenendo al contempo gli usi illeciti e pericolosi in grado di compromettere la pace mondiale a causa di applicazioni letali che, senza peraltro l'intervento umano, possono prendere decisioni in auto-apprendimento con incerte e discriminatorie implicazioni sulla vita delle persone, a maggior ragione in mancanza di un coordinamento sistemico che consenta di sfruttare adeguatamente il potenziale dell'IA mitigandone i rischi a discapito degli individui.

2.7. La fiducia e la sicurezza digitale

Promuovere la "fiducia e la sicurezza digitale" nell'ambito di un dialogo inclusivo globale rientra parimenti tra gli obiettivi prioritari delle Nazioni Unite per ridurre i rischi di vulnerabilità e orientare l'uso delle tecnologie verso il bene comune come indispensabile condizione per la crescita equa e sostenibile della società e dell'economia a fronte di un crescente aumento di frequenti attacchi informatici e campagne di disinformazione online in grado di minare il funzionamento di servizi pubblici erogati alla collettività, sul presupposto che oggi le tecnologie digitali sono alla base di infrastrutture fondamentali.

2.8. La governance digitale

In tale prospettiva, prendendo atto della valenza ancora troppo marginale delle questioni relative all'impatto pervasivo delle tecnologie nell'agenda politica spesso frammentata nell'ambito di svariate lacune degli attuali assetti operativi su cui si fonda il governo della Rete, viene evidenziata la necessità di rafforzare il modello di "cooperazione digitale" migliorandone l'architettura co-decisionale aperta a discussioni globali e inclusivi e, ben oltre le dinamiche dell'attuale approccio consultivo *multi-stakeholder*, mediante la creazione di un organismo dotato di mag-

giore responsabilizzazione che affronti questioni urgenti con poteri efficaci in grado di incidere sull'adozione di politiche pubbliche destinate ad orientare il futuro ecosistema di Internet.

3. Costruire un'architettura più efficace per la governance digitale

Di fronte al mutato scenario virtuale caratterizzante un insidioso ambiente digitale all'insegna del dilagante "lato oscuro" della Rete, il ruolo delle Nazioni Unite sta progressivamente cambiando verso inedite prospettive di maggiore "protagonismo" attivo alla ricerca di soluzioni operative in grado di superare le criticità riscontrate rispetto all'originaria genesi della governance di Internet, con l'intento di rafforzare la partecipazione di tutti gli *stakeholders* anche mediante una chiara definizione di ruoli e di responsabilità per garantire l'effettiva rappresentatività di tutta la comunità della Rete.

In particolare, lo studio del UN-HLPDC indica le funzioni[27] che ogni futura architettura di cooperazione potrebbe svolgere secondo l'enunciazione di una serie di principi[28] alla base di un efficiente meccanismo di governance digitale per superare sei lacune principali:

a) la tecnologia digitale e le questioni di cooperazione digitale rimangono relativamente poco presenti in molte agende politiche nazionali, regionali e globali;
b) vi è una scarsa inclusività dei paesi piccoli in via di sviluppo, delle comunità indigene, delle donne, dei giovani e degli anziani e delle persone con disabilità;
c) il gran numero di meccanismi che coprono le questioni di politica digitale ha reso l'attuale architettura della cooperazione digitale molto complessa e non particolarmente efficace;
d) le politiche vengono ancora prevalentemente elaborate dalle istituzioni nell'ambito di processi decisionali separati con una frammentazione delle strategie aggravata dalla mancanza di comunicazione tra i diversi organismi incompatibile con la configurazione interconnessa della Rete;
e) la mancanza di dati affidabili sull'ecosistema digitale, come fattore indispensabile per realizzare statistiche su cui basare interventi politici pratici;
f) l'assenza di fiducia e collaborazione tra governi, società civile e settore privato, che provoca scarsa comprensione e consapevolezza sulle potenzialità offerte dalle tecnologie.

A fronte di tali sfide, si delineano come utili soluzioni tre possibili alternative[29]:

1. Internet Governance Forum Plus;
2. Distributed Co-Governance Architecture;
3. Digital Commons Architecture.

Il primo propone di implementare l'IGF *multi-stakeholder*. Il secondo identifica un'architettura distribuita che si basa su meccanismi esistenti. Il terzo prevede un approccio "comune" con un coordinamento leggero da parte dell'ONU.

Sebbene nelle soluzioni previste sussistano al contempo benefici e svantaggi[30], è possibile individuare, come elemento positivo comune, l'esigenza prioritaria di valorizzare lo strumento delle consultazioni pubbliche aperte a tutti nell'ottica di favorire il massimo coinvolgimento delle parti.

In particolare il Segretario dell'ONU raccomanda di estendere e trasformare l'Internet Governance Forum (IGF) in un "IGF plus" dotandolo di poteri incisivi, per affrontare le questioni urgenti, coordinare le azioni di follow-up delle discussioni che emergono e condividere con maggiore autorevolezza le proprie raccomandazioni alla pluralità degli attori che operano nel settore sulla base di un'agenda più mirata e limitata alla definizione di specifiche questioni politiche strategiche, che siano di immediato interesse a livello governativo e parlamentare in modo da assicurare risultati più fattibili[31].

La necessità di realizzare un sostanziale rafforzamento del Forum ha origine nelle diverse discussioni politiche e accademiche[32] emerse nell'ultimo decennio che ne criticavano la scarsa apertura come fattore limitante l'efficacia del dialogo fra le parti interessate, con la conseguenza di frenare gli obiettivi perseguiti secondo le raccomandazioni previste dall'agenda di Tunisi[33]: emblematico, al riguardo, il paragrafo 73, che sollecitava l'attivazione di canali di collaborazione tra l'IGF e altri meccanismi di governance del settore pubblico, del settore privato e *multi-stakeholder* per la definizione congiunta e condivisa di questioni e funzioni legate a Internet, al punto da ipotizzare la possibilità di modificare l'Internet Governance Forum (IGF) in un processo di natura decisionale, con la creazione del nuovo organismo – il Multi-Stakeholder High-Level Body (MHLB) – e l'introduzione di un percorso di dialogo intergovernativo e parlamentare secondo un approccio *multi-stakeholder* in grado di aprire la strada a risultati più concreti e tangibili.

Prima di intraprendere qualsiasi azione verso una nuova struttura dell'IGF, l'autorevole CGI.br[34] sostiene che sia necessario eseguire un'analisi più approfondita che possa identificare meglio le lacune attuali così come le attività e le azioni da implementare anche in funzione della creazione di nuove strutture adeguate a fornire soluzioni ai problemi esistenti, per poi ridefinire il mandato di IGF e trasformarlo

in un meccanismo di cooperazione digitale permanente, più orientato ai risultati, e dotato di supporto istituzionale, finanziamenti e personale per essere al passo con le attuali tendenze e problematiche di Internet. Alla luce di tali esigenze, viene rilevata come principale criticità la mancanza di informazioni più dettagliate e di collegamenti tra i problemi esistenti e le potenziali soluzioni che le nuove strutture proposte potrebbero concretamente assicurare[35].

In tale prospettiva, emerge la necessità di predisporre più efficaci meccanismi di negoziazione intergovernativa funzionali all'elaborazione di principi condivisi. Malgrado tali esigenze, si registra nella prassi una crescente divergenza di orientamenti governativi a presidio di interessi "particolari" che compromettono la stabilità sicura ed affidabile di Internet a causa di un'eccessiva frammentazione di interventi politici non sempre del tutto orientati a stimolare l'apertura accessibile e inclusiva della Rete.

Si assiste ad un progressivo indebolimento della democrazia rappresentativa esposta al pericolo del cd. "autoritarismo digitale"[36] che trova terreno fertile in nome della necessità di salvaguardare la sicurezza nazionale di fronte al rischio di una possibile "cyberguerra" che giustifica l'adozione di sofisticati sistemi automatizzati di sorveglianza anche a costo di ridurre la libertà di Internet, reprimendo qualsivoglia critica di dissenso mediante strumenti preventivi di "filtro" e censura. Emblematico, al riguardo, il cd. "Great Firewall"[37] cinese in grado di attuare strategie massive di sorveglianza generale.

Per assicurare la tutela della sicurezza nazionale, è stato realizzato un inedito modello di comonitoraggio multipartecipato attuato mediante una radicata struttura burocratica governativa affiancata da aziende specializzate nel controllo delle informazioni con l'ulteriore supporto di volontari reclutati per monitorare le conversazioni da censurare[38].

In questo senso, la Roadmap, cogliendo la principale criticità dell'attuale ecosistema di Internet, ne traccia l'evoluzione del futuro assetto verso processi concreti di multilateralismo cooperativo, sebbene senza il raggiungimento di un consenso unanime a livello globale, c'è il rischio che i governi nazionali continueranno a muoversi in ordine sparso nello sviluppo disomogeneo di politiche innovative, con il risultato di vanificare la possibilità di dare un'organica visione sistematica al settore che solo la creazione di un'unitaria cabina di regia condivisa dalla comunità internazionale è in grado di assicurare.

Per quanto riguarda "le preoccupazioni che queste proposte possano essere considerate andare oltre la struttura di governance e i mandati originali dell'IGF", riteniamo che andare oltre il mandato e la struttura originali non sia necessariamente un problema, dato che lo sviluppo della tecnologia e della società sono imperativi per la revisione e l'evoluzione dei modelli di governance. Questa evoluzione è in realtà in linea con il paragrafo 73b dell'Agenda di Tunisi, che sottopone la struttura dell'IGF a una revisione periodica. Se è stato identificato che alcuni quadri sono obsoleti o in attesa di miglioramenti, la questione deve essere presa in considerazione, in modo da esaminarla attentamente e apportare i miglioramenti adeguati al modello. Più specificamente, è giusto e ragionevole considerare una modifica del mandato dell'IGF, o anche un'implementazione più esplicita delle pratiche già previste dall'agenda di Tunisi. In particolare, il mandato dell'IGF indica già che potrebbe fare raccomandazioni, se del caso, ma questo non è mai stato messo in pratica, soprattutto per una mancanza di interesse di alcuni gruppi di interesse. In ogni caso, l'ONU dovrà modificare il linguaggio del mandato dell'IGF, in modo da accogliere i ruoli previsti per tutte le strutture che confluiscono nel modello IGF Plus: l'acceleratore di cooperazione, l'incubatore di politiche, l'osservatorio e l'help desk.

Poiché «Internet [...] sta realizzando anche una grande redistribuzione di potere»[39] sembra, quindi, giunto il momento di elaborare innovative politiche multi-stakeholder coordinate a livello internazionale per garantire effettive condizioni di libertà digitale.

Se si vuole evitare il definito sopravvento della "cybersorveglianza", come era massivamente caratterizzata da controlli, censure e manipolazioni è indispensabile presidiare il corretto esercizio di diritti fondamentali, a maggior ragione in uno scenario, come quello attuale, in cui chi, da "player" dominante, raggiungerà il primato egemonico nello "scacchiere" geopolitico globale, riuscendo a dettare le nuove "regole del gioco", sarà in grado di condizionare il complessivo equilibrio di settori che dipendono oggi in larga misura della gestione di Internet.

In caso contrario, le spinte concorrenziali che alimentano il frenetico dinamismo del mercato digitale potrebbero degenerare verso preoccupanti prospettive di guerra commerciale da neo-colonialismo tecnologico[40], con significative ripercussioni destinate ad incidere non solo sull'infrastruttura tecnica della Rete, ma anche e soprattutto sugli standard culturali, economici e sociali del progresso umano.

La forte commistione tra sviluppo sostenibile, sicurezza informatica e crescita produttiva, a fronte delle intense interferenze che si manifestano nell'ambito dell'attuale era digitale, impongono di definire rapidamente una prioritaria strategia di cooperazione globale a presidio dei diritti umani mediante un equilibrato bilanciamento del complesso rapporto

che si instaura tra tecnologia e libertà, con l'obiettivo di investire in generali programmi di alfabetizzazione informatica funzionali ad incrementare la consapevolezza degli utenti sull'uso efficace, sicuro e affidabile del digitale, per evitare che le nuove tecnologie «portino ad una concentrazione invece che ad una diffusione del potere sociale e politico»[41].

4. Considerazioni conclusive

In conclusione, la Roadmap è molto utile perché fornisce molti elementi che sono importanti per le discussioni future a partire dalle attuali mancanze su come migliorare i processi esistenti.

Al netto comunque delle buone intenzioni, sarà decisiva la volontà politica formalizzata da tutte le parti interessate nel percorso di cooperazione da sviluppare per incrementare le attuali dinamiche dell'ecosistema della Rete.

Rispetto al rapido ritmo del cambiamento tecnologico i meccanismi di cooperazione digitale non sono riusciti a tenere il passo; anzi crescono le preoccupazioni ampiamente condivise dalla comunità scientifica, facendo proprie le osservazioni lungimiranti del "maestro" Rodotà, convinto sostenitore del riconoscimento di principi e diritti conformi alla natura globale di Internet come risultato di una partecipazione inclusiva e orizzontale "bottom-up" in grado di coinvolgere la generale comunità degli utenti della Rete, interessati a condividere progetti e proposte di regolazione giuridiche secondo le procedure tipiche del «metodo wiki», superando quindi l'impostazione top-down[42].

Potrebbe, al riguardo, risultare decisivo l'imminente Global Solutions Summit 2021 che si svolgerà in occasione della presidenza italiana del G20. Il Summit sarà aperto da Angela Merkel e Mario Draghi e riunirà i migliori ricercatori, responsabili politici, leader aziendali e rappresentanti della società civile per tentare di risolvere i problemi globali aggravanti dalle dinamiche emergenziali del mondo post-Covid, nell'ottica di legare il progresso economico all'obiettivo di prosperità sociale e la sostenibilità ambientale.

Digital governance, *digital divide*, *digital technologies*, *digital responsibility*, *digital age*: sono alcune parole chiave del programma.

L'auspicio è che si riesca a dialogare superando l'attuale frammentazione dell'ecosistema digitale, mediante l'elaborazione di standard condivisi su cui fondare un innovativo modello di cooperazione digitale efficiente su scala globale.

Note

[1]La cooperazione digitale è «il modo con il quale lavoriamo insieme per affrontare l'impatto sociale, etico, legale ed economico delle tecnologie digitali al fine di massimizzare i loro benefici e minimizzare i loro danni»: cfr. *The Age of Digital Interdependence*, Report of the UN Secretary-General's High-level Panel on Digital Cooperation, June 2019.

[2]Cfr. United Nation, General Assembly, *Road map for digital cooperation*, Report of the Secretary-General, 22 May 2020.

[3]La governance della Rete rappresenta «un elemento essenziale per una società dell'informazione incentrata sulle persone, inclusiva, orientata allo sviluppo e non discriminatoria»: cfr. *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6, p. 31.

[4]Il WSIS, indetto dall'Assemblea Generale delle Nazioni Unite con la risoluzione 56/183 del 21 dicembre 2001, si è svolto nell'ambito di due distinte fasi. La prima fase dei lavori del WSIS di Ginevra (10 al 12 dicembre 2003) si è conclusa con l'emanazione di una "Dichiarazione di principi" e un "Piano d'Azione", che sancisce l'impegno multilaterale coordinato dalle Nazioni Unite (cfr. *Plan of Action*, WSIS-03/GINEVRA/DOC/5-E, Introduction) di costruire una Società dell'Informazione inclusiva superando le condizioni inique di diffusione disomogenea delle tecnologie digitali (cfr. *Declaration of Principles*, WSIS-03/GENEVA/DOC/004, p. 10). La seconda fase a Tunisi (16 al 18 novembre 2005) ha prodotto l'elaborazione del documento *Tunis Commitment*, ove si enuncia l'obiettivo prioritario di colmare il divario digitale mediante l'attuazione di azioni concrete in grado di assicurare la capillare diffusione della cultura digitale (cfr. Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6).

[5]Secondo uno studio UNCTAD del 2014, ci sono più di 680 meccanismi di cooperazione digitale sviluppati e utilizzati da governi, imprese, organizzazioni tecniche e internazionali. Vedi *United Nations Commission Mapping of International Internet Public Policy Issues*, E/CN.16/2015/CRP.2, 17 April 2015.

[6]Si vedano i risultati delle iniziative che seguono. *European Commission's High Level Group on Internet Governance* che ha il ruolo di facilitare la cooperazione fra gli stati dell'Unione europea sulle questione della Internet Governance; *NETmundial Multistakeholder Statement*, Global Multistakeholder Meeting on the Future of Internet Governance del 2014, conosciuto come *NETmundial*, dove si sono discussi due important temi: i principi per la Internet Governance e la Roadmap per l'evoluzione futura della Internet Governance; *One Internet*, il rapporto finale 2016 dei lavori della Global Commission on Internet Governance, è una iniziativa pianificata in due anni per produrre una visione strategica sul futuro della Internet Governance; *Contract for the Web* è il report del World Wide Web Foundation; nel 2018 Francia e Canada hanno avviato un *New Expert International Panel on Artificial Intelligence*; Nel 2016, al Summit G20 è stato adottato il *G20 Digital Economy Development and Cooperation Initiative*; il discorso del Segretario Generale dell'ONU *The Age of Digital Interdependence*, IGF 2018. Molti documenti e pubblicazioni rilasciati nell'ultimo decennio sottolineano la necessità di una migliore inclusione delle comunità sottorappresentate in Internet governance e nei processi di politica digitale. Un esempio è *The report of the Working Group on Improvements to the Internet Governance Forum* del 2012. Anche l'ICANN ha riconosciuto la necessità di una migliore inclusione delle comunità sottorappresentate e sta lavorando per affrontare questo problema attraverso iniziative come il suo *ICANN Fellowship Program*.

[7]Il mandato originale dell'IGF (paragrafo 72, *Agenda di Tunisi*) include due paragrafi relativi alla "cooperazione digitale": 72b. Facilitare il dialogo tra gli organismi che si occupano di diverse politiche pubbliche internazionali trasversali riguardanti Internet e discutere le questioni che non rientrano nel campo di applicazione di nessun organismo esistente. 72c. Interfacciarsi con le organizzazioni intergovernative appropriate. L'idea alla base dei due paragrafi era di creare uno spazio di "discussione" *multi-stakeholder* e collegarlo alle strutture dove si prendono le "decisioni".

[8]Un esempio di successo è il modello decisionale dell'*Internet Engineering Task Force* (IETF) che è l'organismo internazionale, aperto a tutti, composto da tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Si occupa di sviluppare e promuovere standard Internet, in particolare TCP/IP e la *suite* di protocolli Internet, basati sul giudizio degli esperti che partecipano e sulla esperienza di chi la rete la sviluppa e la fa funzionare davvero, implementando le regole specificate dallo IETF stesso. La parola d'ordine del IETF è la collaborazione, il motto è *Rough consensus and running code*, cioè *Consenso diffuso e codice funzionante*: le proposte non vengono adottate con votazioni formali, ma viene richiesto che ricevano un consenso generalizzato all'interno del gruppo di lavoro e che vi siano delle implementazioni funzionanti e diffuse.

[9]L'*Internet Governance Forum* nell'attuale sua costituzione è risultato un meccanismo poco efficace per la cooperazione digitale. Fu convocato per la prima volta nel 2006 ed è un organismo informale che coinvolge tutti gli attori dell'ecosistema della Rete (Stati, istituzioni pubbliche, organizzazioni internazionali, settore privato, e società civile), interessati a discutere sui problemi riguardanti il governo di Internet sulla base di un processo decisionale avente natura non vincolante mediante l'elaborazione di semplici raccomandazioni finalizzate alla condivisione di proposte in un contesto collaborativo, facilitando lo scambio di idee e opinioni. La prima storica edizione dell'IGF globale si è svolta ad Atene (Grecia) nel 2006. Gli eventi successivi sono stati organizzati in numerosi Paesi di tutto il mondo: Rio de Janeiro (Brasile) – 2007; Hyderabad (India) – 2008; Sharm El Sheikh (Egitto) – 2009; Vilnius (Lituania) – 2010; Nairobi (Kenya) – 2011; Baku (Azerbaigian) – 2012; Bali (Indonesia) – 2013; Istanbul (Turchia) – 2014; João Pessoa (Brasile) – 2015; Jalisco (Messico) – 2016; Ginevra (Svizzera) – 2017; Parigi (Francia) – 2018; Berlino (Germania) – 2019; Vitual IGF (ONU) – 2020. Il prossimo IGF globale si terrà dal 6 al 10 dicembre 2021 a Katowice (Polonia).

[10]Cfr. *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6, paragrafo 73. In particolare, dopo l'Agenda di Tunisi istitutiva nel 2005 dell'iniziativa, ne è stato recentemente prorogato il rinnovo per altri successivi 10 anni (2016-2025) secondo quanto stabilito dalla Risoluzione ONU 68/198 del 20 dicembre 2013 approvata in attuazione dei risultati del Vertice mondiale sulla Società dell'Informazione di cui alla Risoluzione ONU 68/31 del 31 luglio 2014.

[11]Si rinvia a L. Abba, A. Alù, *Internet Governance forum: l'evoluzione del modello multi-stakeholder tra criticità e prospettive future*, in questa Rivista, n. 1/2020.

[12]L'obiettivo dell'approccio olistico dei "sistemi" è di riunire enti governativi come le autorità della concorrenza e le agenzie dei consumatori con il settore privato, i cittadini e la società civile per permettere loro di essere più produttivi nel rispondere ai problemi e gestire i compromessi man mano che emergono.

[13]Su tali aspetti si rinvia alle autorevoli osservazioni di W. Kleinwächter, *Internet Governance Outlook 2021: Digital Cacophony in a Splintering Cyberspace*, in "CircleID", 8 January 2021.

[14]Cfr. Resolution adopted by the General Assembly on 21 September 2020 - *Declaration on the commemoration of the seventy-fifth anniversary of the United Nations*, United Nations.

[15]Il panel UN HLPDC è stato istituito nel 2018 per rafforzare la cooperazione internazionale e *multi-stakeholder* e contribuire al dibattito pubblico su un futuro digitale sicuro e inclusivo per tutti. È stato presieduto dalla filantropa Melinda Gates e dal leader dell'e-business Jack Ma. Nel giugno 2019, dopo una serie di incontri di persona dei membri e consultazioni regionali, il Panel ha pubblicato un rapporto intitolato *The Age of Digital Interdependence*. Un processo di *follow-up* del rapporto che coinvolge gli Stati membri delle Nazioni Unite e oltre 300 altre entità (elencate in un allegato al rapporto del Segretario generale) è stato coordinato dal Consigliere speciale del Segretario generale delle Nazioni Unite sui preparativi per la commemorazione del 75° Anniversario dell'ONU.

[16] La composizione del panel rappresentava un ampio *mix* di discipline e settori, nonché una diversità geografica, di genere e di età, come esigenza di integrale rappresentatività del tessuto digitale esistente. Rispetto alla variegata compagine costituita, risulta sintomatica l'assenza di referenti italiani sia come membri del gruppo sia come contributori nelle consultazioni pubbliche (UN-IGF, UN-HLPDC). Tutti i membri hanno prestato servizio a titolo personale, non come rappresentanti delle loro istituzioni affiliate. Co-presidenti: Melinda Gates (USA), Co-Chair of The Bill Melinda Gates Foundation; Jack Ma (China), Executive Chairman, Alibaba Group. Membri: Mohammed Al Gergawi (UAE), Minister of Cabinet Affairs and the Future, UAE; Yuichiro Anzai (Japan), Senior Advisor and Director of Center for Science Information Analysis, Japan Society for the Promotion of Science; Nikolai Astrup (Norway), Minister of Digitalisation, Norway; Vinton Cerf (USA), Vice President and Chief Internet Evangelist, Google; Fadi Chehadé (USA), Chairman, Chehadé Company; Sophie Soowon Eom (Republic of Korea), Founder of Adriel AI and Solidware; Isabel Guerrero Pulgar (Chile), Director, IMAGO Global Grassroots and Lecturer, Harvard Kennedy School; Marina Kaljurand (Estonia), Chair of the Global Commission on the Stability of Cyberspace; Bogolo Kenewendo (Botswana), Minister of Investment, Trade and Industry, Botswana; Marina Kolesnik (Russian Federation), senior executive, entrepreneur and WEF Young Global Leader; Doris Leuthard (Switzerland), former President and Federal Councillor of the Swiss Confederation, Switzerland; Cathy Mulligan (United Kingdom), Visiting Research Fellow Imperial College Centre for Cryptocurrency; Akaliza Keza Ntwari (Rwanda), ICT advocate and entrepreneur; Edson Prestes (Brazil), Professor, Institute of Informatics, Federal University of Rio Grande do Sul; Kira Radinsky (Israel), Director of Data Science, eBay; Nanjira Sambuli (Kenya), Digital Equality Advocacy Manager, World Wide Web Foundation; Dhananjayan Sriskandarajah (Australia), Chief Executive, Oxfam GB; Jean Tirole (France), Chairman of the Toulouse School of Economics and the Institute for Advanced Study in Toulouse.

[17]La *Internet Corporation for Assigned Names and Numbers* con i suoi molteplici comitati consultivi e organizzazioni di supporto può essere vista come un meccanismo di cooperazione digitale istituzionalizzato.

[18]Vedi il video dove i Membri del UN High-level Panel on Digital Cooperation spiegano la necessità di trovare nuovi modi di cooperazione globale per massimizzare i benefici e minimizzare i danni delle tecnologie.

[19]Il documento non è disponibile in lingua italiana.

[20]1. Build an inclusive digital economy and society; 2. Develop human and institutional capacity; 3. Protect human rights and human agency; 4. Promote digital trust, security and stability; 5. Foster global digital cooperation.

[21]Cfr. United Nations, *Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation Report of the Secretary-General*, 29 maggio 2020.

[22]A tal fine, dopo la pubblicazione del rapporto finale elaborato dal gruppo di esperti, è stata prevista l'organizzazione di meeting e tavole rotonde che hanno stimolato la partecipazione di tutti gli *stakeholders* rappresentativi dei settori fondanti la governance della Rete al fine di fornire ulteriori feedback su tali raccomandazioni. L'elenco delle attività e i risultati della consultazione pubblica sono visibili in rete.

[23]Cfr. *Follow-up to the Report of the High-level Panel on Digital Cooperation Roundtable Champions and Key Constituents*, 24 April 2020.

[24]Si rinvia al documento United Nations, *Roadmap for digital cooperation*, cit.

[25]*Ivi*, pp. 5-6.

[26]Sulla base di quanto ipotizzato dal documento World Economic Forum (ed.), *The future of Jobs Report 2020*.

[27]Attingendo anche al lavoro di iniziative precedenti la Road Map suggerisce le seguenti funzioni. "Leadership": generare la volontà politica tra i leader di governo, del mondo degli affari e della società, e fornire una risposta autorevole alle sfide della politica digitale. "Deliberation": fornire un ambiente per prendere decisioni sulle questioni digitali con la partecipazione attiva ed efficace di tutte le parti interessate. "Ensuring inclusivity": assicurare la partecipazione attiva e significativa di tutte le parti interessate, collegandosi con le reti e le iniziative dal basso esistenti e future. "Evidence and data": monitorare gli sviluppi e identificare le tendenze per orientare le decisioni, anche analizzando le fonti di dati esistenti. "Norms and policy making": costruire il consenso tra diverse parti interessate, rispettando il ruolo degli Stati e delle organizzazioni internazionali nel promulgare e far rispettare le leggi. "Implementation": dare seguito alle discussioni e agli accordi politici. "Coordination": creare la consapevolezza e un obiettivo comune tra enti in diverse aree politiche e a diversi livelli (locale, nazionale, regionale, globale), assicurando la sincronizzazione degli sforzi, l'interoperabilità e la coerenza delle politiche, e la possibilità di un coordinamento volontario tra i gruppi di *stakeholder* interessati. "Partnerships": catalizzare i partenariati intorno a questioni specifiche fornendo opportunità per la creazione di reti e la collaborazione. "Support and capacity development": rafforzare lo sviluppo delle capacità, studiando gli sviluppi digitali, identificando le tendenze, informando i decisori politici e il pubblico dei rischi e delle opportunità, e fornendo dati per un processo decisionale basato su prove e permettendo alle persone tradizionalmente emarginate o ad altre parti interessate con meno risorse di partecipare attivamente al sistema. "Conflict resolution and crisis management": sviluppare le competenze, conoscenze e strumenti per prevenire e risolvere le controversie e assistere le parti interessate in caso di crisi.

[28]Sono individuati i seguenti principi chiave. "Consensus-oriented": Le decisioni dovrebbero essere prese in modo da cercare consenso tra gli *stakeholder* pubblici, privati e della *civil society*. "Polycentric": Il processo decisionale dovrebbe essere altamente distribuito basato sulle capacità con un coordinamento blando ma efficace. "Customised": Non c'è generalmente una soluzione "unica per tutti"; diverse comunità possono implementare le norme a modo loro, secondo le circostanze. "Subsidiarity": Le decisioni dovrebbero essere prese il più localmente possibile, il più vicino a dove si trovano le questioni e i problemi. "Accessible": Dovrebbe essere facile e possibile per tutti impegnarsi nei meccanismi di digitale e e partecipare alle discussioni politiche. "Inclusive": Le decisioni dovrebbero essere inclusive e democratiche, rappresentando interessi diversi e ragionevoli nei confronti di tutte le parti interessate. "Agile": La cooperazione digitale dovrebbe essere dinamica, iterativa e capace di rispondere rapidamente alle questioni politiche che emergono vai via. "Clarity in roles and responsibility": Ruoli chiari e linguaggio comune dovrebbero ridurre la confusione e sostenere la comprensione comune sulle responsabilità degli attori coinvolti nella cooperazione digitale (governi, settore privato, società civile, organizzazioni internazionali e università). "Accountable": Ci dovrebbero essere risultati misurabili, responsabilità e strumenti per ricorrere. "Resilient": La distribuzione del potere dovrebbe essere bilanciata tra i settori, senza controllo centralizzato dall'alto verso il basso. "Open": I processi dovrebbero essere trasparenti, con barriere minime all'entrata. "Innovative": Dovrebbe essere sempre possibile innovare nuovi modi di cooperare, dal basso verso l'alto, che è anche il modo migliore per includere prospettive diverse. "Tech-neutral": Le decisioni non dovrebbero bloccare tecnologie specifiche ma permettere l'innovazione di alternative migliori e adeguate al contesto. "Equitable outcomes": La cooperazione digitale dovrebbe massimizzare l'interesse pubblico globale interesse pubblico globale (a livello internazionale) ed essere ancorata ad un ampio beneficio pubblico (a livello nazionale).

[29]Il primo migliora ed estende l'IGF *multi-stakeholder*. Il secondo è un'architettura distribuita che si basa su meccanismi esistenti. Il terzo prevede un approccio "comune" con un coordinamento lasco da parte dell'ONU. Tutti hanno benefici e svantaggi. Sono presentati nella Road Map per fornire punti di partenza concreti per l'ulteriore discussione e l'ampia consultazione che il Gruppo UN-HLPDC ha raccomandato al Segretario generale dell'ONU.

[30]Cfr. *The Age of Digital Interdependence*, Report of the UN Secretary-General's High-level Panel on Digital Cooperation, June 2019, p. 24.

[31]Cfr. United Nations, *Roadmap for digital cooperation*, cit., paragrafi 93-96. §93. Mentre le discussioni sui diversi modelli di architettura digitale proposti dal Panel sono in corso tra le parti interessate, le seguenti idee sono emerse al fine di rendere l'Internet Governance Forum più reattivo e pertinente alle attuali questioni digitali. Queste includono: (a) Creare un organismo strategico *multi-stakeholder* di alto livello e dotato di poteri, basato sull'esperienza dell'attuale gruppo consultivo *multi-stakeholder*, che affronti questioni urgenti, coordini le azioni di follow-up delle discussioni del Forum e trasmetta gli approcci politici proposti e le raccomandazioni del Forum ai forum normativi e decisionali appropriati; (b) Avere un'agenda più mirata per il Forum basata su un numero limitato di questioni politiche strategiche; (c) Stabilire un segmento di alto livello e percorsi ministeriali o parlamentari, che assicurino risultati più fattibili; (d) Creare legami più forti tra il Forum globale e le sue iniziative regionali, nazionali, subregionali e giovanili; (e) Integrare con maggiore efficacia il programma e il lavoro di sviluppo politico intersessionale per sostenere altre aree prioritarie delineate nel presente rapporto; (f) Affrontare la sostenibilità a lungo termine del Forum e le risorse necessarie per una maggiore partecipazione, attraverso una strategia di raccolta fondi innovativa e percorribile, come promosso dalla tavola rotonda; (g) Migliorare la visibilità del Forum, anche attraverso un'identità aziendale più forte e una migliore attività di reporting alle altre entità delle Nazioni Unite. §94. Mentre le consultazioni sui modelli di architettura digitale continueranno nei prossimi mesi, sostengo queste misure per migliorare il Forum e intendo attuarle in quanto opportune. §95. In questo momento senza precedenti, il potere, la promessa e il pericolo della tecnologia digitale non possono essere sottovalutati. Unirsi permetterà alla comunità internazionale di assicurare che la tecnologia sia sfruttata per il bene, di cercare l'opportunità di gestire il suo impatto e di garantire che presenti condizioni di parità per tutti. §96. Le generazio-

ni future giudicheranno se la generazione presente ha colto le opportunità presentate dall'era dell'interdipendenza digitale. Il tempo di agire è ora.

[32]Tra cui UN Commission on Science and Technology for Development, *Report of the Working Group on Improvements to the Internet Governance Forum*, 2012; M. Mueller, B. Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, in "Internet Policy Observatory", 2014, n. 2; Internet Governance Forum, *IGF Retreat Proceedings: Advancing the 10-Year Mandate of the Internet Governance Forum*, 2016; W. Kleinwächter, *The Start of a New Beginning: The Internet Governance Forum on Its Road to 2025*, in "CircleID", April 3, 2016; R. Echeberría, *Let's Reform the IGF to Ensure Its Healthy Future Internet Society*, 2018.

[33]L'Agenda di Tunisi precisa: «The report has also enhanced our understanding of the respective roles and responsibilities of governments, intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries.» *Ivi*, paragrafo 33 «Diverse matters relating to Internet governance would continue to be addressed in other relevant fora». *Ivi*, paragrafo 79.

[34]L. Abba, A. Lazzaroni, *Il Comitato di gestione per l'Internet istituito dal Governo del Brasile*, in "Informatica e Diritto", 2013, n. 2, pp. 167-182.

[35]Cfr. Brazilian Internet Steering Committee – CGI.br (ed.), *Comments to the proposed IGF Plus model*. Il CGI.br pur sostenendo l'IGF come un forum prezioso per la discussione di "questioni di politica pubblica relative agli elementi chiave della governance di Internet al fine di promuovere la sostenibilità, la solidità, la sicurezza, la stabilità e lo sviluppo di Internet", raccomanda di allargare e promuovere la cooperazione tra soggetti diversi in una prospettiva globale.

[36]R. Kemeny, *Brasil is sliding into techno-authoritiananism*, in "MIT – Technology Review", 19 August 2020.

[37]G.R. Barme, S. Ye, *The Great Firewall of China*, in "Wired", 6 January 1997.

[38]Si veda il Report *Freedom on the Net 2019*, secondo cui in Cina si commettono le peggiori violazioni della libertà di Internet a causa di livelli di censura "senza precedenti".

[39]S. Rodotà, *Parlamenti e sviluppo della società dell'informazione*, in Internet Society Italia (a cura di), "Quaderni dell'Internet italiano", 27 settembre 2007.

[40]Sul tema si rinvia alle osservazioni di W. Kleinwächter, *Internet Governance Outlook 2021: Internet Governance Outlook 2021*, cit.

[41]S. Rodotà, *Parlamenti e sviluppo della società dell'informazione*, cit.

[42]S. Rodotà, *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3.

* * *

Current shortcomings and future solutions in digital cooperation mechanisms

Abstract: The new *Roadmap for Digital Cooperation* of the UN Secretary General represents a true milestone. It is the outcome of the Internet organisations' work to redesign the digital cooperation ecosystem. Taking into account the impact of the COVID-19 pandemic on our society, the roadmap highlights the critical gaps and challenges that the Internet governance is facing, as well as illustrates the possible path to strengthen the worldwide digital cooperation by enhancing the stakeholder participation in the Internet Governance Forum. In the past, the World Summit on Information Society, WSIS, was the only intergovernmental mechanism to discuss public policy matters related to the Internet. At present, there are more informal and formal ways and forums for such purpose that surround the United Nations environment. Acknowledging the key role that Internet plays at worldwide level, it is of paramount importance to pursue international synergies to tackle the digital governance matters and to overcome the current deadlock that prevents the revamping of existing mechanisms.

Keywords: Global connectivity – Digital public goods – Digital inclusion – Digital capacity building – Digital human rights – Artificial intelligence – Digital trust and security – Global digital cooperation

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0034

Democrazia come *Value-Sensitive Design*: un approccio sociotecnico allo sviluppo delle tecnologie basate su principi democratici

Kelvin Peroli • Cíntia Rosa Pereira de Lima

Sin dall'avvio delle riflessioni di Norbert Wiener sulla cibernetica negli anni Cinquanta del secolo scorso, il fenomeno dell'interconnessione dei dispositivi informatici ed anche dello sviluppo delle reti è stato collegato ad elementi di analisi non solo tecnici, ma anche sociali. In questa direzione, l'articolo propone riflessioni sulla democrazia come un valore umano che necessita di essere sintetizzato in tecnologie che, a loro volta, sono piattaforme di reti di comunicazione, nelle ipotesi in cui queste tecnologie siano destinate a rispecchiare il sistema sociale presente nel mondo offline. Perciò, lo studio adotta l'ottica di un design sensibile ai valori umani (*Value-Sensitive Design*). L'analisi è esemplificata con l'applicazione *Bridgefy*, che è stata utilizzata, nel 2020, in diverse proteste in tutto il mondo, come nel movimento *Black Lives Matter* e nelle proteste contro la rielezione del presidente della Bielorussia, Aleksandr Lukashenko.

Democracy by Design – *Value-Sensitive Design* – Interazione uomo-macchina – Approccio sociotecnico della democrazia

Sommario: *1. Introduzione – 2. Sistemi sociotecnici – 3.* Value-Sensitive Design *– 4.* Democracy by Design *– 5.* Democracy by Design *nel 2020: l'app* Bridgefy *e il suo uso nel movimento* Black Lives Matter *e nelle proteste contro Aleksandr Lukashenko, presidente della Bielorussia – 6. Conclusioni*

1. Introduzione

"Le macchine sviluppate dall'uomo possono imparare e riprodursi?"[1]

A partire come base da questa domanda del cibernetico Norbert Wiener (1961), le riflessioni di questo articolo hanno l'obbiettivo, inizialmente, di fare alcune considerazioni sulle risposte alle seguenti domande (che sono già state messe in discussione, in maniera concettuale, in ottica sociotecnica, da Jeremy Pitt, Andrew Jones ed Alexander Artikis[2]): nello sviluppo del design dei sistemi, gli sviluppatori sono veramente coscienti dei concetti che stanno ad inserire (per input) in un modello informatico? Sono, in realtà, coscienti delle scelte che il modello avrebbe l'autonomia di adottare? Le risposte sono, molte volte, assolutamente negative. Queste sono domande (essenzialmente tipiche della sociologia e della *cybersociology*) che dimostrano l'importanza della comunicazione tra i sistemi sociale e tecnologico nella costruzione delle tecnologie – ad esempio, che siano capaci di pensare o agire come l'uomo (oppure *per* l'uomo). Di conseguenza, in quest'ipotesi, il processo dello sviluppo delle tecnologie (oggi basate, soprattutto, sull'Intelligenza Artificiale – IA) richie-

K. Peroli è laureato in Giurisprudenza all'Università di São Paulo (Brasile), con *academic exchange* svolto all'Università degli Studi della Campania Luigi Vanvitelli. C.R. Pereira de Lima è professoressa associata di Diritto civile presso l'Università de São Paulo (Brasile), con post dottorato in Giurisprudenza presso l'Università degli Studi di Camerino e dottorato di ricerca presso l'Università di São Paulo, con stage di ricerca svolto all'Università di Ottawa (Canada). Il primo è associato fondatore dell'*Instituto Avançado de Proteção de Dados* (Istituto Avanzato di Protezione Dati) – IAPD, la seconda, oltre a essere associata fondatrice, ne è presidente.

de l'osservanza dei valori umani (sintetizzati sui dispositivi) che possono interferire sulla performance delle stesse. Questo approccio tecnico è noto come *Value-Sensitive Design* (VSD).

Ignorare valori e principi nel *design* delle tecnologie è, propriamente, aumentare il rischio di pregiudizi (*bias*) nel momento del funzionamento delle macchine.

Per questo motivo, queste riflessioni intendono dimostrare come la democrazia (come definita da Jeremy Pitt e Josiah Ober[3]) può essere implementata già dall'origine e dalla pianificazione delle tecnologie (*by design*), in modo che, partendo da una analisi sociotecnica, abbia come scopo, di volta in volta, la costruzione di sistemi tecnologici che pongano pari attenzioni alle componenti tecniche e sociali.

L'analisi di un ipotetico uso della *Democracy by Design* (DbD) è esemplificata con l'app *Bridgefy* – che è stata utilizzata, in anni recenti, in una serie di proteste (nel 2020, ad esempio, nelle proteste contro la rielezione del presidente della Bielorussia, Aleksandr Lukashenko, e nel movimento *Black Lives Matter*, negli Stati Uniti). Questa app rappresenta, di per sé, sia l'uso della tecnologia (e delle reti sociale) nell'esercizio della democrazia, sia l'uso di una tecnologia in cui sono inseriti, teoricamente, i valori (o i principi) della *Democracy by Design*.

2. Sistemi sociotecnici

Uno dei principali obiettivi dell'evoluzione tecnologica è, certamente, l'aumento dell'efficienza delle organizzazioni e dei sistemi (come comunità online, reti sociali).

La tecnologia, in sua visione guidata dallo studio dell'interazione tra uomo e macchina (*human-machine interaction*), è evoluta, soprattutto, nel secondo dopoguerra, nel momento in cui la comunicazione (tra esseri umani, tra esseri umani e macchine ed anche soltanto tra macchine) è stata definita come oggetto di studio della Cibernetica e, pochi anni dopo, dell'Intelligenza Artificiale[4].

L'approccio iniziale dell'IA[5], in questo contesto, aveva un paradigma di ragionamento *simbolico* (ossia, dell'uso, nelle macchine, di uno linguaggio di rappresentazioni con simboli), mentre la Cibernetica, si può dire, aveva un paradigma di ragionamento connessionista (ovvero l'utilizzazione del modello cerebrale nel suo oggetto di studio – che era la comunicazione e il controllo degli animali, società e macchine). Questo approccio del connessionismo è stato introdotto nell'IA, soprattutto a metà degli anni Ottanta del secolo scorso[6], quando l'impiego del solo ragionamento simbolico si è rivelato inefficiente per coprire tutti i tipi di sviluppi nell'IA. All'epoca, il paradigma *brain-oriented* è stato compreso con il termine connessionismo, che già esisteva, almeno, dalla concezione del modello probabilistico di archiviazione e organizzazione d'informazione negli umani e nelle macchine di Frank Rosenblatt, il *Perceptron*[7].

Dallo studio del rapporto tra macchine e umani, è stato osservato (concettualmente, da Fred Emery, Eric Trist e Ken Bamforth, ancora negli anni 1950)[8] che l'utilizzazione delle machine per l'aumento dell'efficienza e della produttività delle organizzazioni (ossia, l'impiego di un sistema tecnico) aveva bisogno, in realtà, della comunicazione della tecnologia con il tipo di struttura sociale di una data organizzazione (compresi i suoi valori e bisogni), in modo da effettuare l'ottimizzazione degli obiettivi da essa perseguiti (in questo caso, efficienza e produttività).

Quindi, a questa struttura (comprese le sue relazioni con le persone) è stato assegnato il sostantivo "sociale", mentre all'insieme tecnologico utilizzato in un dato sistema o organizzazione è stato attribuito il sostantivo "tecnico". Dunque, lo studio della comunicazione (oppure della interazione) tra questi due sottosistemi (sociale e tecnico) è stato inteso come *socio-technical system* – sistema sociotecnico.

Da un punto di vista sociotecnico, l'interazione tra umani e machine è effimera (o liquida – in riferimento a Zygmunt Bauman[9]) perché il modo di pensare degli umani (ad esempio, i suoi valori ed obiettivi) cambia costantemente.

In questo senso, il modo in cui gli esseri umani pensano e comunicano dovrebbe essere catturato nella progettazione (design) dei sistemi tecnologici, malgrado questo non significhi che, a causa di nuovi aggiornamenti (*updates*), le impostazioni (*by design*) non possano essere modificate, nel futuro.

Si può dire, infatti, che la prospettiva sociotecnica è un'analisi dell'interazione tra gli strati che compongono una tecnologia (come un dispositivo con l'IA), che è composta, in questo senso, da uno strato meccanico (hardware), da uno strato informazionale (software), da uno umano (*human-machine* oppure *human-computer interaction*) ed ancora un altro sociale (network).

Il design, quindi, deve comprendere sia gli aspetti tecnici che sociali, in modo che la comunicazione tra questi elementi sia adeguatamente prestabilita (*by design*) dagli sviluppatori, mitigando il rischio di pregiudizi (*bias*) imprevisti (mitigando, perciò, il *socio-technical gap*). Pertanto, qualsiasi tecnologia che abbia, in qualche modo, prestabilito l'analisi su queste componenti, è, in una certa misura, un sistema sociotecnico.

In proposito, si considerino, ad esempio, i social network (come Facebook, Instagram, Twitter e Wikipedia), i motori di ricerca (come Google, Bing e Yahoo), le piattaforme di *e-commerce* (come Amazon), l'e-mail (Gmail e Microsoft Outlook), il World Wide Web e l'ipermedia, i browser Web (Google Chrome, Safari, Mozilla Firefox e Microsoft Edge) ed i servizi di streaming (Spotify, Amazon Prime Music e Video, Netflix e Deezer). Tutti questi esempi impiegano tecnologie (hardware + software) che interagiscono tra loro (*machine* + *machine*) e con gli utenti (*human* + *machine*), e che sono anche, allo stesso tempo, piattaforme che mediano la comunicazione tra i suoi utenti (*human* + *human* = social)[10].

Rudolph Oosthuizen e Carien Van't Wout sottolineano, per questo motivo, che il *design* dei sistemi sociotecnici può essere implementato da almeno tre prospettive: (i) *human-centred perspective* (in una visione antropocentrica, in cui la tecnologia deve essere un supporto per il processo decisionale); (ii) *team-oriented perspective* (la tecnologia come parte del *team*, avendo l'importante ruolo della *fiducia* nelle relazioni tra suoi membri – umani e macchine); e (iii) *work-oriented perspective* (con il *focus* nell'analisi del lavoro che deve essere implementato dal team – umani e macchine)[11].

Dopo l'analisi delle prospettive che possono essere scelte nel *design* dei sistemi, è ancora importante definire gli attributi qualitativi (*valori* o *principi*) che devono essere implementati. Questa analisi è il cosiddetto *Value-Sensitive Design* (VSD).

3. *Value-Sensitive Design*

La creazione di un sistema sensibile ai valori umani e sociali (*Value-Sensitive Design*), secondo Batya Friedman, Peter Kahn e Alan Borning, è un approccio che impiega attributi qualitativi (valori o principi) ai requisiti primari di un sistema (tecnologico), come pure ai requisiti funzionali e non-funzionali[12].

La cura verso i valori umani nelle macchine è stata discussa principalmente da Norbert Wiener, che si è interessato, soprattutto, della protezione della sicurezza (dell'uomo) e delle opportunità di lavoro, a fronte della crescente automazione del lavoro.

Ignorare i valori durante il design di un sistema non è, in realtà, privarlo di attributi qualitativi. Quando si costruisce un sistema (nell'ipotesi di mancato rispetto di valori e principi), le scelte sono necessariamente arbitrarie e implementate dagli sviluppatori, che le articolano con valori e pregiudizi (*bias*) su cui si sono basati. Negli anni Novanta, questa idea è stata elaborata sul software, in particolare da Friedman, Terry Winograd, Ben Shneiderman[13] e Helen Nissenbaum.

Nissenbaum e Introna, ad esempio, hanno analizzato i motori di ricerca (*search engines*), che già avevano, all'epoca, i *bias by design*: «Il nostro studio sui motori di ricerca suggerisce che essi escludono sistematicamente (in alcuni casi in base alla progettazione ed in alcuni accidentalmente) alcuni siti e alcune tipologie di siti a favore di altri, sistematicamente evidenziando alcuni a scapito di altri. Sosteniamo che tali pregiudizi, che porterebbero ad un restringimento del funzionamento del Web nella società, sono in contrasto con l'architettura di base del Web, nonché con i valori e gli ideali che hanno alimentato un supporto diffuso per la sua crescita e sviluppo»[14].

La tecnica, in effetti, tiene conto dei valori durante la fase del design, affinché rimangano efficaci per tutto il ciclo di vita del sistema. Uno degli esempi più noti è il principio della *Privacy by Design* (PbD), che sostiene la privacy (ed anche, di fatto, la protezione dei dati personali) come un attributo qualitativo da essere considerato già nella fase del design dei sistemi.

Il *design*, in tal senso, è una forma di potere: una forma di potere degli sviluppatori sugli utenti, come già aveva affermato Woodrow Hartzog[15] – dalla metafora di Michel Foucault del sistema panottico di Jeremy Bentham, è il grado di opacità della torre di sorveglianza (quello che decide se i prigionieri sapranno oppure no di essere sorvegliati). Quindi, il design, già dall'inizio, dovrebbe essere permeato di buone pratiche – ad esempio, con la protezione della privacy (*Privacy by Design*) –, al fine di aiutare a mitigare lo spettro della sorveglianza (e non più rafforzare l'immagine purtroppo realistica dell'uomo di vetro, come direbbe ancora Rodotà)[16].

A titolo illustrativo, come definito da Ann Cavoukian[17], ci sono sette principi fondamentali per sviluppare una tutela della privacy (e dei dati personali) già dalla progettazione:

i. *Proactive not reactive, preventive not remedial* – "dovrebbe esserci una preferenza per la prevenzione dei rischi, piuttosto che per porvi rimedio";
ii. *Privacy as the default setting* – "privacy come una impostazione di *default*";
iii. *Privacy embedded by design* – "privacy incorporata dal design";
iv. *Full functionality – positive-sum, not zero-sum* – "piena funzionalità del prodotto o servizio con l'impostazione della *privacy by design* e *by default* (ossia, la funzionalità non dovrebbe essere completamente disponibile soltanto a coloro che mitigano l'impostazione della privacy)";

v. *End-to-end security – full lifecycle protection* – "protezione durante tutto il ciclo di vita del trattamento dei dati personali";
vi. *Visibility and transparency – keep it open* – "visibilità e trasparenza";
vii. *Respect for user privacy – keep it user-centric* – "rispetto per la privacy del titolare dei dati personali".

4. *Democracy by Design*

Al di là dell'approccio alla *privacy* e alla protezione dei dati, molti altri valori sono stati e sono in fase di studio e sistematizzazione – per la loro rispettiva applicazione in un dato tipo di sistema.

In questa direzione, Jeremy Pitt e Josiah Ober[18] hanno sistematizzato l'applicazione dell'attributo "democrazia" in sistemi aperti (cioè, sistemi che interagiscono con l'ambiente). L'hanno chiamata "democrazia di base", intrisa di principi in grado di mitigare i rischi di alterazione d'una situazione democratica (precedentemente configurata) in un'autocrazia, un'oligarchia oppure in una tirannia della maggioranza[19], nei sistemi (o piattaforme) in cui è inserita.

Pitt e Ober hanno sostenuto che la "democrazia di base", a differenza della democrazia liberale, è intesa come un sistema di *empowerment*, processo decisionale (*decision-making*) e azione (*action*), basato, infatti, sulla capacità di tutti i cittadini di fare, selezionare, modificare, applicare e far rispettare le regole.

Sulla base di questa premessa, sono state effettuate simulazioni con l'uso di un sistema sociotecnico intelligente[20], in un ambiente virtuale (creato con il nome di *Demopolis*), al fine di dimostrare come i sistemi aperti, basati sui principi della "democrazia di base", possano mitigare i suddetti rischi.

Pertanto, secondo Pitt e Ober, l'attributo della *Democracy by Design* è considerare la "democrazia di base" già dall'inizio, nella progettazione di un sistema sociotecnico aperto, in cui questo attributo qualitativo (valore oppure principio) deve consentire agli utenti di auto-organizzarsi nel sistema, senza consentire che tale potere venga trasferito a pochi utenti o solo ai proprietari della piattaforma considerata. Questo potere può essere inteso come una *governance* algoritmica, in cui un insieme di regole predetermina le possibili future azioni degli sviluppatori e degli utenti, limitandoli ad agire, a sua volta, soltanto secondo le regole, cioè, ad agire in conformità.

Sulla base delle simulazioni effettuate, Pitt e Ober hanno proposto otto principi fondamentali di una *Democracy by Design*:

i. *Prevention rather than re-invention* - "Prevenzione piuttosto che reinvenzione" significa che le caratteristiche che possono far degenerare un sistema democratico dovrebbero, idealmente, essere previste e non rimediate.
ii. *Democracy is not an end-state, nor the default* - La "democrazia non come fine, né come default, ma in base alla progettazione" (*by design*) è la necessità di monitorare e proteggere la democrazia in ogni momento, non soltanto in alcuni intervalli di tempo oppure solo come un obbiettivo ancora da perseguire, essendo possibile che gli utenti stessi monitorino il sistema, il cui sforzo può essere compensato.
iii. *Democracy embedded in design* – La "democrazia incorporata alla progettazione" (*by design*), in questo senso, assicura che le regole di procedura per le deliberazioni democratiche e per il processo decisionale siano consolidate dalla concezione o progettazione del sistema, invece di cercare di consolidarle soltanto quando il progetto è stato finalizzato.
iv. *No compromises on democratic processes* - "Non danneggiare i processi democratici" significa, di fatto, che nessun *trade-off* può sovrapporsi di fronte alla democrazia.
v. *Visibility, inclusivity, transparency and accountability* - La "visibilità" significa, a sua volta, che il riconoscimento (ad esempio, fatti e contenuti) deve essere visibile ed accessibile. "L'inclusione", a sua volta, è la necessità che la democrazia debba essere sempre perseguita al massimo, per includere veramente tutti. La "trasparenza" e "l'accountability" sono descritte come azioni che dovrebbero essere sempre intraprese dai decisori (*decision-makers*) e dagli utenti del sistema. Per quanto riguarda la *accountability*, è necessario che i decisori possano sempre essere identificati e ritenuti responsabili delle loro azioni.
vi. *Inter-dependence of diversity* - L'"interdipendenza della diversità" è uno strumento per la stabilità del sistema, poiché la democrazia è composta da forze diverse e spesso antagoniste, che però può produrre un sistema più o meno stabile, a seconda dei "controlli e contrappesi" applicati.
vii. *Education in the recognition of prosocial benefits* - "Educazione al riconoscimento dei benefici sociali" significa riconoscere "l'effimero" (la transitorietà) degli utenti, cioè garantire che anche i nuovi utenti possano conoscere i vantaggi della partecipazione nel sistema, ma anche, in alcuni casi, verificare o indagare circa la legittimità delle autorità di un dato sistema e consentire che

queste possano essere indubbiamente contestate e modificate. Infine

viii. *Procedural evaluation* - L'"analisi e valutazione dei procedimenti utilizzati" è la necessità di giudicare le procedure di selezione, applicazione e interpretazione delle regole, e anche di saper accogliere la pluralità delle regole e di conciliare i conflitti che ne derivano.

5. *Democracy by Design* nel 2020: l'app *Bridgefy* e il suo uso nel movimento *Black Lives Matter* e nelle proteste contro Aleksandr Lukashenko, presidente della Bielorussia

L'utilizzo della comunicazione da parte dei social network come forma di organizzazione di resistenza è cresciuto nel decennio del 2010, con la diffusione, soprattutto, degli *smartphone*. La Primavera araba, nel 2011, è uno dei principali esempi della lotta per la democrazia con l'uso di strumenti di connessione e creazione di comunità.

In questo contesto, Hosni Mubarak ha disconnesso l'Egitto da Internet il 28 gennaio 2011[21], disattivando 3.500 prefissi degli IPs (*Internet Protocols*) egiziani. Questo ha significato l'interruzione della comunicazione dei prefissi con il *routing* effettuato per protocolli di rotta (*Border Gateway Protocols* – *BGPs*), che collegano, a loro volta, i provider di servizi Internet (ISP) egiziani con altri paesi – e che consentono di trasferire pacchetti di dati agli IP che hanno il prefisso[22].

Milioni di utenti sono stati disconnessi in pochi minuti (tra le 22:12 e le 22:35 p.m. – ora del Cairo). L'11 febbraio 2011, invece, è stato segnato dalla caduta del regime di Mubarak (al potere per 30 anni) attraverso una rivoluzione rafforzata dai social network.

All'epoca dello shutdown, Google e Twitter hanno offerto l'applicazione *Speek-2-Tweet*, con cui gli utenti potevano chiamare un numero di telefono internazionale nell'intento di inviare e visualizzare *tweets*, anche senza Internet[23].

Questa offerta di opzioni per l'interazione tra le tecnologie ed i suoi utenti, in un contesto sociopolitico come quello della Primavera araba, è uno strumento utile per stabilire una resistenza – in questo caso, democratizzante.

Al di là di questo punto di analisi, però, l'interazione offerta da *Democracy by Design*, come proposta da Pitt e Ober, può raggiungere anche il livello strutturale delle tecnologie.

In questa direzione, la *mesh network* (*rete mesh*) è uno degli esempi di strutture in grado di accoglierla pienamente, in quanto si tratta di un'infrastruttura di rete che collega diversi *nodes* (o *routers*) in modo diretto e non gerarchico, ed anche che può essere utilizzata con o senza le altre architetture di interconnessione (come *Ethernet* e *Wi-Fi*). In questa rete, il protocollo di *routing* seleziona il percorso (in base ai *nodes* di rete disponibili), mirando a un flusso di dati più efficiente.

Attualmente, le reti *mesh* sono utilizzate su scala locale, perché i *nodes* devono stare vicini tra loro affinché i dati possano fluire. Esistono diversi software che utilizzano questa tecnologia, come Briar, FireChat, Bluetooth Low Energy Mesh Networking e *Bridgefy*[24].

Quest'ultimo è un'applicazione che consente agli utenti di creare la propria rete *mesh*[25], anche permettendole di comunicare con l'uso del Bluetooth, a qualsiasi scala, purché vi siano *nodes* (ovvero i dispositivi degli utenti) che interconnettono il flusso.

Questo tipo di connessione è, a seconda del contesto, utile o forse dannosa, in quanto rende difficile per lo Stato il monitoraggio dei pacchetti di dati – una rete *mesh* può non essere controllata da un provider di servizi Internet, ma dagli utenti (perché è non gerarchica e, per questo motivo, distribuita). In ogni caso, è uno strumento che può essere ampiamente utilizzato laddove Internet non è accessibile a tutti o laddove il suo utilizzo è pericoloso.

Effettivamente, questo è stato il caso della Bielorussia, che è rimasta senza connessione Internet dal 9 all'11 agosto 2020, dopo la controversa rielezione del presidente Aleksandr Grigorievitch Lukashenko contro Svetlana Tikhanovskaya: tra le forme di comunicazione usate dai manifestanti, (contrari all'elezione di Lukashenko – considerata da molti una frode) vi è l'app *Bridgefy*.

Dal 2019, l'*app* è stata utilizzata anche per altre proteste, ad esempio a Hong Kong[26] in occasione delle proteste contro un disegno di legge sull'estradizione verso Stati con i quali Hong Kong non ha accordi in materia (compresa la Cina) ed anche usata negli Stati Uniti, nelle proteste *Black Lives Matter*[27].

Nel movimento *Black Lives Matter* del 2020, iniziato con la morte di George Floyd, per asfissia causata da compressione al collo e alla schiena, a Minneapolis il 25 maggio, dopo che il poliziotto Derek Chauvin aveva premuto il ginocchio sul collo di Floyd per 8 minuti e 46 secondi[28], l'applicazione è stata usata in momenti in cui mancava la connessione ad Internet, anche per la sicurezza degli utenti e per la paura di rappresaglie da parte delle autorità nel caso di indagini sui manifestanti. All'e-

poca, però, l'app non aveva ancora comunicazioni completamente crittografate.

L'utilizzo delle reti *mesh* è, come esposto in precedenza, una tecnologia su cui può essere ancora implementata l'ipotesi di *Democracy by Design* di Pitt e Ober. L'app *Bridgefy* si presenta, in quest'analisi, con un carattere illustrativo (poiché i principi della *Democracy by Design* di Pitt e Ober non sono stati considerati *ab initio – by design*). Tuttavia, l'app ha già molti degli attributi della *DbD*, in particolare la "Prevenzione piuttosto che reinvenzione", la "Democrazia incorporata alla progettazione" e "L'inclusione". Inoltre, è uno strumento per promuovere la democrazia, come è stato usato nelle proteste negli Stati Uniti e in Bielorussia.

6. Conclusioni

L'implementazione dei valori e dei principi umani nelle tecnologie è una questione di necessità e adeguatezza: ogni applicazione ha specificità che richiedono, di volta in volta, diversi attributi qualitativi (come riflessioni e punti di vista) per il processo decisionale ed il funzionamento efficace dei sistemi tecnologici intelligenti, in modo che siano, quindi, privi di *bias* non programmati.

Tra questi valori vi è la *Privacy by Design*. Al di là della privacy, vi sono poi la tensione verso la democrazia e la sua "*pulsione di ripudio*" del totalitarismo, nelle sue diverse modalità, dall'autocrazia e oligarchia alla tirannia della maggioranza. Sia la *privacy* sia la *democrazia* sono in grado di mitigare la visione panottica di sviluppatori di tecnologie sugli utenti ed anche di offrire sistemi, di conseguenza, con scenari più partecipativi e trasparenti.

La *Democracy By Design*, come idealizzata da Pitt e Ober (e simulata, attraverso un'analisi sociotecnica, in realtà virtuale – la *Demopolis*), è stata esemplificata con l'app *Bridgefy*, per la ragione che è in grado di rappresentare, di per sé, come affermato, sia l'uso della tecnologia per l'esercizio della democrazia sia l'uso della tecnologia con valori democratici – incorporati *by design*.

Note

[1] «Can man-made machines learn and can they reproduce themselves?». N. Wiener, *Cybernetics or the control and communication in the animal and the machine*, II ed., MIT Press, 1961, p. 170.

[2] M.R. Albrecht, J. Blasco, R. Bjerg Jensen, L. Marekova, *Mesh Messaging in Large-scale Protests: Breaking Bridgefy*, 2020.

[3] J. Pitt, J. Ober, *Democracy by Design: Basic Democracy and the Self-Organization of Collective Governance*, in Proceedings of the "IEEE 12th International Conference on Self-Adaptive and Self-Organizing Systems" (Trento, 3-7 September 2018), p. 20-29.

[4] R. Oosthuizen, C. Van't Wout, *Sociotechnical System Perspective on Artificial Intelligence Implementation for a Modern Intelligence System*, in Proceedings of the "24th International Command and Control Research & Technology Symposium", 2019, 13 p.

[5] Sulla creazione del termine Intelligenza Artificiale (in contrasto con la Cibernetica), John McCarthy ha dichiarato: «One of the reasons for inventing the term 'artificial intelligence' was to escape association with 'cybernetics'. Its concentration on analog feedback seemed misguided, and I wished to avoid having either to accept Norbert (not Robert) Wiener as a guru or having to argue with him». J. McCarthy, *Defending AI Research: A Collection of Essays and Reviews*, Center for the Study of Language and Information, 1996, p. 225.

[6] Günther Hoffmann si è occupato dell'origine del connessionismo nell'Intelligenza Artificiale: «In the mid-1980s a renaissance of neural networks took place under the new title of connectionism, challenging the dominant symbolic paradigm of AI. The 'brain-oriented' connectionist paradigm claims that research in the traditional symbolic paradigm cannot be successful since symbols are insufficient to model crucial aspects of cognition and intelligence. Since then a debate between the advocates of both paradigms is taking place, which frequently tends to become polemic in many writings on the virtues and vices of either the symbolic or the connectionist paradigm. Advocates on both sides have often neither appreciated nor really addressed eachothers arguments or concerns». A.G. Hoffmann, *Paradigms of Artificial Intelligence: a methodological and computational analysis*, Springer-Verlag, 1998.

[7] Rosenblatt sviluppò il "Perceptron" negli anni 1950 e lo pubblicizzò nel 1958 come un tipo ipotetico di sistema nervoso oppure di macchina. F. Rosenblatt, *The Perceptron: a probabilistic model for information storage and organization in the brain*, in "Psychological Review", 1958, n. 6, p. 386-408.

[8] Il sistema sociotecnico (STS) è un approccio del "work design" che include, nel suo sistema, l'interazione tra persone e tecnologia. Il termine è nato con Eric Trist, Fred Emery e Ken Bamforth, dai loro studi presso il *Tavistock Institute* di Londra, con i lavoratori delle miniere di carbone. B. Friedman, P.H. Kahn jr., A. Borning, *Value Sensitive Design and Information Systems*, in Himma K.E., Tavani H.T. (eds.), "The Handbook of Information and Computer Ethics", John Wiley & Sons, 2008, p. 69-101.

[9] Cfr. Z. Bauman, *Modernidade Líquida*, Zahar, 2001.

[10] B. Whitworth, A. Ahmad, *The Social Design of Technological Systems - Building Technologies for Communities*, II ed., Interaction Design Foundation, 2014.

[11] R. Oosthuizen, C. Van't Wout, *op. cit.*

[12] Al riguardo, Friedman, Kahn Jr. e Borning: «Value Sensitive Design is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process». B. Friedman, P.H. Kahn jr., A. Borning, *op. cit.*

[13] Cfr. B. Shneiderman, *Leonardo's Laptop, Human Needs and the New Computing Technologies*, MIT Press, 2002.

[14] «Our study of search engines suggests that they systematically exclude (in some cases by design and in some, accidentally) certain sites and certain types of sites in favor of others, systematically giving prominence to some at the expense of others. We argue that such biases, which would lead to a narrowing of the Web's functioning in society, run counter to the basic architecture of the Web as well as to the values and ideals that have fueled widespread support for its growth and development». L.D. Introna, H. Nissenbaum, *Shaping the*

Web: Why the Politics of Search Engines Matters, in "The Information Society", 2000, n. 16, p. 169-185.

[15] «Design is power because people react to design in predictable ways. This means that with the right knowledge, design can impose some form of order on chaos». W. Hartzog, *Privacy's Blueprint - The Battle to Control the Design of New Technologies*, Harvard University Press, 2018, p. 34.

[16] Rodotà ha avvertito dell'impatto dell'"uomo di vetro" sul cyberspazio già negli anni 1990: «'L'uomo di vetro' è metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi». S. Rodotà, *Relazione annuale 1997*, Garante per la Protezione dei Dati Personali, 1998.

[17] A. Cavoukian, *Privacy by Design - The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2011, 2 p.

[18] «Basic democracy has been proposed as a means of collective self-governance distinct from liberal democracy, i.e. it is a conventional rule-based system of empowerment, decision-making and public action that is both prior to and separate from concerns such as justice, morality and rights». J. Pitt, J. Ober, *op. cit.*

[19] La tirannia della maggioranza è intesa come una deviazione dal senso di democrazia. Può essere definita dalla seguente citazione di Alexis de Tocqueville (che deve essere interpretata, tuttavia, nel contesto dei suoi studi sulla democrazia degli Stati Uniti, nel XIX secolo): «Quando dunque io rifiuto di obbedire ad una legge ingiusta, non nego affatto alla maggioranza il diritto di comandare: soltanto mi appello non più alla sovranità del popolo ma a quella del genere umano». A. Tocqueville, *A Democracia na América - Leis e Costumes*, Martins Fontes, 2005, p. 294.

[20] «The method starts with an engineering problem to solve; observing how people or communities solve similar problems; formalising a theory (from the social sciences) of those observations in a calculus of preference (logic, game theory, etc.); implementing a computational model; experimenting with that model; then evaluating if this is a solution to the original problem». J. Pitt, J. Ober, *op. cit.*, p. 21.

[21] N. Cohen, *Egyptians Were Unplugged, and Uncowed*, in "The New York Times", Feb. 21, 2011.

[22] «What BGP does is 'advertise' the local address prefixes to neighbouring networks. Wholesale ISPs propagate their customer's advertisements to their neighbours so that eventually all ISPs know all other ISPs' prefixes. This enables routers to know where to send packets with a given destination address. The 3,500 Egyptian prefixes are now no longer advertised, so they're missing from the routing tables of BGP routers around the world. This means that routers no longer know where to send packets addressed to IP addresses that fall within these prefixes—even if all the cables are still working fine». I. van Beijnum, *How Egypt did (and your government could) shut down the Internet*, in "Ars Technica", 2011.

[23] C.A. Frangonikolopoulos, I. Chapsos, *Explaining the role and impact of social media in the Arab Spring*, in "Global Media Journal", Mediterranean Edition, 2012, VII ed., v. 2, p. 11-20.

[24] M.R. Albrecht, J. Blasco, R. Bjerg Jensen, L. Marekova, *op. cit.*, punto 2.

[25] *Ibidem.*

[26] J. Koetsier, *Hong Kong Protestors Using Mesh Messaging App China Can't Block: Usage Up 3685%*, in "Forbes", 2019.

[27] «The Bridgefy developers report uptake of Bridgefy during the Black Lives Matter protests across the United States of America». M.R. Albrecht, J. Blasco, R. Bjerg Jensen, L. Marekova, *op. cit.*, punto 2.

[28] E. Hill, A. Iefenthäler, C. Triebert et al., *How George Floyd Was Killed in Police Custody*, in "The New York Times", May 31, 2020.

* * *

Democracy as a Value-Sensitive Design: a sociotechnical approach to the development of technologies based on democratic principles

Abstract: At least since Norbert Wiener's cyber circle (in the 1950s), the phenomenon of the interconnection of computer devices and the development of networks has been linked to elements of analysis that are not only technical, but also social. Within this context, this study proposes reflections on democracy as a human value that need to be synthesized in technologies that are, in this sense, communication network platforms, in the hypothesis of the technologies themselves (and their developers) aim to reflect online the social system present in the offline world. Therefore, the present research adopts the perspective of a design that is sensitive to human values (Value-Sensitive Design). This analysis is exemplified with the app *Bridgefy*, which was used globally in 2020 in various protests, such as in the "Black Lives Matter" movement and in the protests against the re-election of the Belarusian president, Aleksandr Lukashenko.

Keywords: Democracy by Design – Value-Sensitive Design – Human-computer interaction – Socio-technical approach to democracy

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0029

Roberto Zaccaria, Alessandra Valastro, Enrico Albanesi, *Diritto dell'informazione e della comunicazione* XI edizione, Milano, Wolters Kluwer-Cedam, 2021

Enrico Albanesi

La recensione delinea in modo sintetico ed argomentato quello che costituisce il filo rosso sotteso alla undicesima edizione del manuale R. Zaccaria, A. Valastro, E. Albanesi, *Diritto dell'informazione e della comunicazione*, Milano, Cedam-Wolters Kluwer, 2021. Un'analisi critica, cioè, del principio costituzionale del pluralismo (elaborato in Italia dalla giurisprudenza costituzionale con riguardo alla radiotelevisione a partire dagli anni Settanta/Ottanta), così come ancora oggi emergente dalla giurisprudenza della Corte costituzione e delle Corti europee con riguardo al nuovo ambiente tecnologico venutosi ad affermare con la rivoluzione digitale e la trasformazione della rete Internet, specie a partire dalla seconda metà degli anni Duemila. Un principio purtroppo ancora oggi incompiuto nella sua realizzazione pratica in Italia.

1. Si tratta dell'undicesima edizione di un Manuale nato nel 1996 sulla base dell'esperienza universitaria ed arricchitosi via via anche dell'esperienza pratica. L'attuale edizione si divide in tre parti. La Parte I è dedicata a delineare, con l'ausilio di dottrina e giurisprudenza, specie costituzionale ed europea, il quadro costituzionale della libertà di informazione e di comunicazione in Italia e dei loro limiti, a partire dagli artt. 21 e 15 Cost. La Parte II ha ad oggetto gli organi di governo del sistema (Parlamento, Governo ed Agcom) e la disciplina delle reti di comunicazione elettronica (in generale e, nello specifico, della rete Internet) e dei soggetti di rete (quali, a seconda dei diversi servizi, i fornitori di rete, i c.d. intermediari di rete o i fornitori di servizi audiovisivi). La Parte III si concentra sulle varie normative settoriali riguardanti la RAI, l'editoria, la professione giornalistica, il riparto di competenze tra Stato e Regioni, la disciplina *antitrust*, il cinema, il teatro ed il diritto d'autore.

2. Quello dell'informazione e della comunicazione in Italia rappresenta un settore nel quale prevalgono forti interessi di parte e che non ha ancora raggiunto l'indispensabile consolidamento dei principi. Di fronte ad un quadro normativo così articolato e complesso, uno dei motivi conduttori del volume è sempre stato la verifica dello stato di attuazione del principio pluralistico, che costituisce il risvolto positivo del diritto all'informazione garantito dall'art. 21 Cost., che nella società contemporanea è il vero diritto di accesso alle fonti della conoscenza e quindi alla cittadinanza. Un principio elaborato in Italia dalla Corte costituzionale a partire dagli anni Settanta/Ottanta del secolo scorso con specifico riferimento al settore radiotelevisivo. Era infatti in particolare il settore radiotelevisivo che, alla luce della scarsità delle frequenze che caratterizzava l'etere quale mezzo trasmissivo, richiedeva che fossero garantite, da un lato, la possibilità d'ingresso nel mercato radiotelevisivo del maggior numero possibile di soggetti consentiti

R. Zaccaria, già professore ordinario di Istituzioni di diritto pubblico presso l'Università di Firenze, è stato, prima, consigliere (1977-1993) e successivamente presidente della RAI (1998-2002). A. Valastro è professore associato di Diritto pubblico presso il Dipartimento di Scienze politiche dell'Università di Perugia. E. Albanesi è professore associato di Diritto costituzionale presso il Dipartimento di Giurisprudenza dell'Università di Genova.

dai mezzi tecnici (pluralismo esterno); dall'altro, la diffusione, da parte della concessionaria pubblica, di quante più possibili opinioni, tendenze, correnti di pensiero politiche, sociali e culturali presenti nella società (pluralismo interno).

In particolare, l'interrogativo di fondo di quest'edizione del Manuale, a venticinque anni dalla sua prima edizione, è verificare se l'esigenza costituzionale di garantire il principio pluralistico sia ancora attuale. A primo acchito, la risposta sembrerebbe negativa: la rivoluzione digitale, il processo di convergenza multimediale e lo sviluppo capillare in particolare della rete Internet hanno condotto ad incrementare le potenzialità di accesso per nuovi soggetti al sistema dell'informazione e delle comunicazioni, come mai avvenuto in passato. Il passaggio al digitale terrestre, con il c.d. *switch off* nel 2012 ha moltiplicato il numero di canali televisivi e dunque effettivamente realizzato un pluralismo tecnico. Alcuni siti Internet, o comunque taluni *blog* personali che trattano temi di attualità (da quelli politici a quelli sociali ed economici), hanno acquisito progressivamente autorevolezza, rappresentando sempre più spesso una fonte d'informazione alternativa rispetto a quella dei *media* cartacei o radiotelevisivi c.d. *mainstream*: una "galassia" di contenuti che rappresenta una ricchezza per la circolazione delle idee e per la libertà e pluralità dell'informazione. Tanto da condurre la Corte di Cassazione a riconoscere un ruolo essenziale nella società democratica al "giornalismo diffuso" sulla rete Internet nonché una tutela pari a quello professionale, almeno dal punto di vista dei principi costituzionali coinvolti[1].

3. La rivoluzione digitale, il processo di convergenza multimediale e soprattutto la trasformazione più recente della rete Internet hanno tuttavia posto nuove sfide dal punto di vista costituzionale. Ebbene, la risposta all'interrogativo di cui sopra, che emerge dallo studio condotto nell'attuale edizione del Manuale, è che il principio pluralistico costituisce ancora un'esigenza costituzionale meritevole di tutela nell'ambiente digitale che caratterizza l'attuale sistema dell'informazione e della comunicazione: tanto da essere ancora ben presente nella recente elaborazione giurisprudenziale della Corte costituzionale ed ora financo delle Corti europee.

3.1. Quanto alla Corte costituzionale, basti pensare alla sentenza n. 206 del 2019, dove la Corte, dopo aver richiamato la propria giurisprudenza in materia di pluralismo, ha ribadito il valore centrale del principio in un ordinamento democratico, «fino al punto da giustificare ed anzi imporre al legislatore interventi idonei a garantirne il rispetto»[2]. Dal canto suo, la Corte di giustizia dell'Unione europea, nel caso *Vivendi*, nel 2020 ha dichiarato la contrarietà al diritto dell'Unione europea di criteri aprioristici riguardanti precise soglie di ricavi di imprese esercenti attività di comunicazione, fissati da una legislazione come quella italiana in materia di *antitrust*, poiché tali soglie, «non consentendo di determinare se e in quale misura un'impresa sia effettivamente in grado di influire sul contenuto dei media, non presentano un nesso con il rischio che corre il pluralismo dei media»[3]. E non può non ricordarsi come qualche anno prima, nel 2012, anche la Corte europea dei diritti dell'uomo nel caso *Centro Europa 7* aveva condannato l'Italia, osservandosi come «in una società democratica, non basta, per garantire un vero e proprio pluralismo nel settore audiovisivo, prevedere l'esistenza di più canali o la possibilità teorica per i potenziali operatori di accedere al mercato audiovisivo. Bisogna anche permettere un accesso effettivo a tale mercato, in modo da assicurare nel contenuto dei programmi globalmente considerati una diversità che rispecchia per quanto possibile la varietà delle correnti di pensiero che attraversano la società alla quale tali programmi sono rivolti»[4].

3.2. L'avvento del digitale terrestre in Italia ha dimostrato quanto le affermazioni della Corte EDU fossero vere. Se infatti il c.d. *switch off* del 2012 ha effettivamente creato dal punto di vista tecnico maggiori potenzialità d'accesso al sistema dell'informazione, per tutta una serie di ragioni la normativa italiana ha consentito che anche nel nuovo sistema si perpetuassero in qualche modo il ruolo preponderante dei gruppi RAI e Mediaset e l'elevato tasso di concentrazione del sistema stesso. Elemento, quest'ultimo, che costituisce un fattore di rischio per il pluralismo dei media nel nostro Paese, come peraltro segnalato nel 2020 dal *Report* del *Centre for Media Pluralism and Media Freedom* dello *European University Institute* di Fiesole[5].

Basti ricordare a tal proposito il modo in cui è stata costruita in Italia la normativa antitrust: imperniata su un paniere del Sistema Integrato delle Comunicazioni (SIC), ai fini del calcolo del limite del venti per cento dei ricavi, del tutto eterogeneo; e su un limite tecnico, riguardante il numero dei canali, del tutto inadeguato, il quale non include quelli a pagamento e non tiene conto del peso specifico di ciascun canale in ragione della posizione sul telecomando ai sensi del piano di numerazione degli stessi.

Ed un ruolo in proposito ha svolto anche l'assenza di una adeguata normativa che risolvesse l'annoso problema del conflitto d'interessi nel nostro Paese, segnalato dalla Commissione europea nel suo *Rapporto sullo Stato di diritto in Italia* ancora nel 2020[6].

In questo quadro, non ha certo aiutato neppure l'inazione dell'Agcom, l'Autorità chiamata a vigilare in materia. Tanto da suscitare perplessità il fatto che (peraltro, *comme d'habitude* in questo settore, con una normativa-ponte della durata di sei mesi) la "risposta" da parte dell'Italia alla sopra citata sentenza sul caso *Vivendi* sia consistita nel 2020 nell'attribuzione all'Agcom del compito di verificare la sussistenza di effetti distorsivi o di posizioni comunque lesive del pluralismo nel caso in cui un soggetto operi contemporaneamente nei mercati delle comunicazioni e in un mercato diverso, ricadente nel SIC[7].

3.3. Che l'avvento della rivoluzione digitale abbia posto nuove sfide dal punto di vista del principio del pluralismo è d'altronde dimostrato dalle perplessità che suscita l'attuale "tenuta" della normativa in materia di propaganda politica e pluralismo informativo, adottata in Italia più di vent'anni fa[8]. Per certi versi, al di là del fatto che dal punto di vista della tecnica legislativa appare più che mai opportuna una sorta di codificazione in materia, tale normativa appare ancora attuale: non essendo ancora venute meno nel nostro Paese quelle condizioni di fatto che secondo la Corte costituzionale[9] giustificano una legislazione in materia di *par condicio* nell'accesso al mezzo radiotelevisivo, mezzo che continua a svolgere un ruolo di fatto dominante nella fruizione di informazioni da parte dell'opinione pubblica[10]. Per altri versi, sembra trattarsi di una normativa ormai inadeguata a regolamentare fenomeni nuovi e completamente diversi che accadono nell'ambiente delle piattaforme digitali. Tale ambiente non presenta invero le stesse problematiche tecniche di accesso al mezzo radiotelevisivo. Tuttavia resta essenziale che sia comunque assicurato ad esso un accesso in condizioni di imparzialità ed equità, con modalità trasparenti e non discriminatorie; e che esso sia regolamentato attraverso strumenti di coregolamentazione o autoregolamentazione, garantendosi in particolare la trasparenza dei contenuti politici online sponsorizzati, come da *Codice di condotta europeo* del 2018[11], da *Linee guida* e *Impegni* promossi dall'Agcom nel 2018 e 2019 attraverso un Tavolo tecnico[12], da *Piano d'azione per la democrazia europea* del 2020[13] o da *Raccomandazioni* in corso di elaborazione in sede di Consiglio d'Europa[14]. Peraltro precondizione a ciò è che, come si nota nel menzionato *Piano d'azione*, si monitorino le attuali norme nazionali in materia di diversità e concentrazione dei media, anche digitali[15].

3.4. Ma forse, più in generale, la sfida più impegnativa deriva dal fenomeno che maggiormente ha trasformato l'ambiente digitale stesso (per come lo si conosceva tra la fine degli anni Novanta ed i primi anni Duemila): la dissociazione, cioè, tra soggetti che gestiscono le reti di comunicazione elettronica (c.d. *telco*) e soggetti che agiscono al di sopra delle reti (c.d. *over-the-top* – OTT). Fenomeno, questo, che ha condotto al superamento di una visione "romantica" della rete Internet ed al passaggio da una decentralizzazione quasi atomistica degli attori, operanti su essa, ad una forte centralizzazione in capo a poche piattaforme digitali globali. Quella "galassia" di contenuti, che rappresenta una ricchezza per la circolazione delle idee e per la libertà e pluralità dell'informazione ed alla quale si è fatto sopra riferimento quale riflesso positivo dell'avvento della rete Internet, ha finito dunque per essere in qualche modo oggi "gestita" in via prioritaria, appunto, da poche piattaforme digitali globali, divenute ormai una sorta di agorà digitale. Dal punto di vista giuridico, è chiaro come tutto ciò chiami di nuovo in ballo *mutatis mutandis* il principio del pluralismo, da declinarsi però in questo caso financo su scala normativa (quantomeno) europea, data la dimensione globale del fenomeno.

Da un lato, in questo quadro, appare cruciale ripensare il tema dell'accesso alla rete Internet (si vedano in particolare da questo punto di vista le novità in tema di servizio di accesso adeguato alla banda larga come servizio universale a prezzo accessibile contenute nella direttiva recante codice europeo delle comunicazioni elettroniche del 2018[16]; nonché quello della c.d. neutralità della Rete, senza che però ciò produca effetti discriminatori tra l'una e l'altra piattaforma digitale o pregiudichi l'utente finale nell'effettività del godimento dei suoi diritti di accesso alla Rete ed ai servizi offerti per il suo tramite.

Dall'altro, sorge l'esigenza di introdurre strumenti di autoregolamentazione o coregolamentazione per contrastare fenomeni quali la c.d. disinformazione, il discorso d'odio in Rete o i contenuti illeciti o nocivi per i minori. La trasformazione delle piattaforme digitali ha infatti condotto queste ultime ad assumere una fisionomia sempre meno passiva e neutrale rispetto ai contenuti veicolati attraverso esse, finendo ciò per mettere in dubbio le tradizionali categorie di inquadramento dei c.d. intermediari di rete nella società dell'informazione di cui alla direttiva sul commercio elettronico del 2000[17] ed alla normativa interna di attuazione del 2003[18]. Nell'ultimo quindicennio la difficile opera di sussunzione di nuove e multiformi fattispecie concrete emergenti da tale quadro tecnologico in evoluzione è stata affidata alla soluzione giurisprudenziale in sede europea (si pensi ai casi *Promusicae*, 2008; *Google France*, 2010; *Scarlet*, 2011; *L'Oreal*, 2011; *Sabam*, 2012; *Google Spain*, 2014; *UPC Telekabel*, 2014; *Papasavvas*, 2014; *Mc Fadden*, 2016; *Eva Glawischnig-Piesczek*, 2019) e nazionale (tra tutte, si pensi a *Google-Vivi Down*, 2010-

2013). Più di recente l'Unione europea è però finalmente intervenuta a livello normativo, introducendosi una disciplina delle piattaforme di condivisione video nella nuova direttiva servizi di media audiovisivi (2018)[19] e dei prestatori di servizi di condivisione online nella direttiva sul diritto d'autore nel mercato unico digitale (2019)[20]. Con tale normativa europea si è così cercato di trovare un punto di caduta che facesse salve la libertà d'espressione, da un lato, e la tutela della dignità umana, dall'altro.

4. Inutile aggiungere che per tutti questi fini, risulta oggi più che mai essenziale che venga rafforzata l'indipendenza delle Autorità Nazionali di Regolamentazione del settore delle comunicazioni (nel nostro Paese, l'Agcom), come peraltro le due direttive del 2018 sopra menzionate richiedono espressamente agli Stati membri.

La nuova direttiva sui media audiovisivi include, tra gli obiettivi di tale rafforzamento, che i poteri dell'Autorità siano esercitati in modo imparziale e trasparente, tra l'altro, per quanto attiene al pluralismo dei media ed impone agli Stati di definire, per la nomina e rimozione dei membri delle Autorità, condizioni e procedure trasparenti, non discriminatorie e che garantiscano il grado di indipendenza richiesto.

Altrettanto rilevante è quanto impone la direttiva recante codice europeo delle comunicazioni elettroniche, la quale obbliga gli Stati a promuovere la stabilità delle competenze dell'Autorità al momento del recepimento della direttiva stessa.

5. In definitiva le sfide che all'Italia si pongono sul versante della tutela del principio del pluralismo sono oggi di due tipi. Da un lato, vi è la necessità di porre mano definitivamente ed in modo strutturale ad alcuni tradizionali nodi irrisolti del sistema dell'informazione: l'annoso conflitto di interessi; la necessità di introdurre una seria normativa *antitrust*, cogliendosi magari l'occasione offerta dalla necessità di dare una "risposta" a regime al caso *Vivendi*; l'urgenza di mettere mano ad una sorta di codificazione della normativa in materia di comunicazione politica e pluralismo informativo; il carente grado di indipendenza dell'Agcom. Dall'altro, si pone ora la necessità di dare attuazione alla normativa europea del 2018/2019 in materia di piattaforme digitali[21], veicolo attraverso cui si potrà peraltro incidere su uno degli annosi nodi sopra menzionati: quello del rafforzamento dell'indipendenza dell'Agcom, come richiesto espressamente dalle due direttive europee del 2018. È pur vero che le Camere hanno appena approvato la legge di delegazione europea 2019-2020[22], recante, tra l'altro, delega al Governo per l'attuazione delle direttive europee che qui rilevano. Tuttavia, ai fini dell'effettiva realizzazione del principio del pluralismo, sarà cruciale vedere il modo in cui il Governo italiano darà attuazione ai principi e criteri direttivi della legge di delegazione europea nell'adozione dei rispettivi decreti legislativi e su ciò sarà opportuno che nel Paese si accendano i riflettori dell'opinione pubblica e si compia un attento monitoraggio da parte della comunità scientifica. Senza peraltro tralasciarsi di verificare le ulteriori novità normative che potrebbero essere adottate in sede europea, ove andassero in porto le proposte, avanzate dalla Commissione europea, di regolamento *Digital Services Act* e *Digital Markets Act* del dicembre 2020[23].

Sotto tutti questi punti di vista, l'auspicio è che l'edizione 2021 del Manuale possa rammentare al decisore pubblico la persistente importanza di assicurare l'effettiva attuazione del principio del pluralismo che, lungi dall'essere magicamente risolto con il progresso della tecnologia digitale, resta ancora essenziale garantire *mutatis mutandis* anche nel nuovo ambiente digitale.

Note

[1]Cfr. Cassazione penale, sezione V, sentenza 25 luglio 2008, n. 31392.

[2]Cfr. Corte costituzionale, sentenza 25 luglio 2019, n. 206, punto 6 del *Considerato in diritto*.

[3]Cfr. Corte di giustizia dell'Unione europea (Quinta Sezione), sentenza 3 settembre 2020, C-718/18, *Vivendi S.A. c. AGCOM e Mediaset*, paragrafo 79.

[4]Cfr. Corte europea dei diritti dell'uomo (Grande Camera), sentenza 7 giugno 2012, ricorso n. 38433/09, *Centro Europa 7 e Di Stefano c. Italia*, paragrafo 130.

[5]Cfr. E. Brogi, R. Carlini, *Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania and Turkey in the years 2018-2019. Country report: Italy*, European University Institute, 2020, p. 13 s.

[6]Cfr. Commissione europea, *Relazione sullo Stato di diritto 2020. Capitolo sulla situazione dello Stato di diritto in Italia*, SWD (2020) 311 final, p. 14.

[7]Cfr. art. 4-*bis*, decreto-legge 7 ottobre 2020, n. 125, convertito con modificazioni in legge 27 novembre 2020, n. 159.

[8]Cfr. legge 22 febbraio 2000, n. 28, *Disposizioni per la parità di accesso ai mezzi di informazione durante le campagne elettorali e referendarie e la comunicazione politica*.

[9]Cfr. Corte costituzionale, sentenza 7 maggio 2002, n. 155, punto 2.2 del *Considerato in diritto*.

[10]Cfr. Agcom, *Rapporto sul consumo di informazione*, 2018.

[11]Cfr. European Commission, *EU Code of Practice on Disinformation*, October 2018.

[12]Cfr. Agcom, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018* e Id., *Impegni assunti dalle società esercenti le piattaforme on line per garantire la parità di accesso dei soggetti politici alle piattaforme digitali durante la campagna elettorale per le elezioni dei membri del Parlamento europeo spettanti all'Italia – 2019*.

[13]Cfr. Commissione europea, *Sul piano d'azione per la democrazia europea*, Comunicazione COM (2020) 790 final, paragrafo 2.1., 3 dicembre 2020.

[14]Cfr. Council of Europe – Committee of experts on media environment and reform (MSI-REF), *Draft recommendation of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns*, 29 March 2021.

[15]Cfr. Commissione europea, *Sul piano d'azione per la democrazia europea*, cit., paragrafo 3.4.

[16]Cfr. Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che *istituisce il codice europeo delle comunicazioni elettroniche*.

[17]Cfr. Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*.

[18]Cfr. decreto legislativo 9 aprile 2003, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico*.

[19]Cfr. Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 *recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato*.

[20]Cfr. Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio del 17 aprile 2019 *sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE*.

[21]In assenza della quale la Commissione europea ha peraltro avviato due procedure d'infrazione nei confronti (tra gli altri) dell'Italia. Cfr. n. 2020_0533 e n. 2021_0056.

[22]Cfr. legge 22 aprile 2021, n. 53, *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2019-2020*.

[23]Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico di servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, 15 dicembre 2020, COM (2020) 825 final e Id., *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*, 15 dicembre 2020, COM (2020) 842 final.

* * *

Abstract: The review focuses on the common thread running through the eleventh edition of the handbook R. Zaccaria, A. Valastro, E. Albanesi, *Diritto dell'informazione e della comunicazione*, Milano, Cedam-Wolters Kluwer, 2021, i.e. a critical analysis of the constitutional principle of pluralism. The principle was established in Italy by the Constitutional Court from the 1970s/1980s with regard to the television broadcasting system. The Constitutional Court, the European Court of Justice and the European Court of Human Rights still refer to it in their case law, with regard to the digital environment born from the digital revolution and the transformation of the Internet from the second half of the 2000s. The handbook argues that the implementation of the principle is still unsatisfactory, though.

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0032

Recensione a: Gianluigi Fioriglio, *Informatica medica e diritto. Un'introduzione*, Modena, Mucchi Editore, 2020

Alessio Facciorusso

Negli anni Settanta del Novecento molti sono stati coloro che hanno visto nell'informatica un valido strumento per migliorare, velocizzare e talvolta automatizzare alcuni significativi processi in campo medico.

D'altra parte, il flusso informativo che lega i diversi soggetti coinvolti nell'ambito sanitario è da tempo decisamente corposo. Si pensi solamente alle informazioni che il medico e il paziente sono soliti scambiarsi vicendevolmente e all'attenzione che viene posta alla conservazione, all'invio e alla ricezione delle stesse, tanto in presenza quanto a distanza, al fine di assicurare il raggiungimento dei molteplici obiettivi previsti dalla relazione clinica. La scienza medica, perciò, non ha potuto fare a meno di essere attratta dall'informatica e dalle sue potenziali applicazioni pratiche, specie in considerazione dei numerosi progressi già compiuti in altri campi.

All'epoca delle prime sperimentazioni, appunto qualche decennio fa, alcuni tra i primi risultati non si rivelarono soddisfacenti per una serie di ragioni.

Innanzitutto, l'intenzione di voler automatizzare diverse procedure in campo medico si scontrò quasi subito con un contesto che non si poteva ancora considerare culturalmente preparato.

Secondariamente, le macchine e i software presenti all'epoca apparivano forse ancora piuttosto limitati rispetto a quelle che erano le aspirazioni di chi, per esempio, già immaginava un computer in grado di sostituire la figura del medico in maniera integrale, dall'analisi fino alla prognosi.

Oltretutto, i primi tentativi di questo genere vennero fatti senza considerare pienamente quali potessero essere le ripercussioni dal punto di vista etico sul rapporto medico-paziente. Il rischio che si sarebbe potuto presentare sarebbe stato quello di una pregiudizievole dematerializzazione della profonda relazione di fiducia che tende ad instaurarsi tra il professionista sanitario e la figura del paziente che, di volta in volta, vi si rivolge.

A distanza di poco più di quarant'anni, la situazione appare sensibilmente diversa. Miliardi di individui possiedono uno o più dispositivi elettronici portatili e interconnessi, senza menzionare la miriade di dispositivi "intelligenti" che abitano le case, gli uffici e altri spazi pubblici e privati. La rivoluzione digitale sembra procedere in maniera inarrestabile, contraddistinta dal dominio dell'informazione nella sua forma dematerializzata.

L'ambito della salute è stato anch'esso investito dai numerosi cambiamenti che tale rivoluzione ha portato con sé, primo fra tutti la digitalizzazione dei sistemi sanitari nel loro complesso, ma anche l'utilizzo dell'intelligenza artificiale e dei Big Data per una gestione sempre più efficace di una mole di dati, quelli relativi ai pazienti e non solo, che vengono ogni giorno raccolti in tutto il mondo. Dunque, l'informatica medica – oggetto della recente pubblicazione di

A. Facciorusso è dottore in Giurisprudenza, laureato presso l'Università degli studi di Modena e Reggio Emilia con una tesi in Informatica giuridica. Attualmente collabora con l'Officina Informatica del CRID (Unimore) - Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità.

Gianluigi Fioriglio – risulta un ambito a cui dedicare particolare e specifica attenzione.

Essa viene definitiva nel volume come la «scienza interdisciplinare che si occupa dello studio e dell'applicazione dell'informatica a ogni ambito della salute» e come tale ha raggiunto un elevato grado di diffusione nella nostra quotidianità, tanto da superare i confini della ricerca accademica o della sola implementazione (e del successivo sviluppo) da parte dei professionisti sanitari.

Oggi, il ricorso agli strumenti e alle applicazioni dell'informatica medica alimenta un dibattito che ha per oggetto numerose questioni etiche e giuridiche, le quali diventano sempre più significative e, senza dubbio, urgenti via via che il numero dei soggetti coinvolti aumenta, unitamente all'eterogeneità degli stessi. Per poter affrontare tale dibattito occorre disporre degli strumenti idonei alla risoluzione degli interrogativi che propone, e pertanto diviene fondamentale il tipo di approccio da adottare.

A tale proposito, il volume propone di individuare e utilizzare una metodologia che si avvalga di strumenti e prospettive proprie dell'Informatica giuridica.

L'obiettivo dell'opera, dunque, è quello di indagare l'informatica medica e tutti i quesiti giuridici e non giuridici che solleva attraverso un approccio che sia strettamente legato anche ad una riflessione giusfilosofica in materia bioetica (p. 10).

L'intero primo capitolo funge come inquadramento delle tematiche centrali della materia (pp. 13-40). Ciò non potrebbe prescindere da un'esauriente illustrazione dell'evoluzione storica dell'informatica medica, elaborata da Fioriglio fin dalle prime pagine del volume.

L'Autore afferma di voler distinguere, da una parte, tra quelli che definisce *requisiti obbligatori* e *requisiti raccomandati* e, dall'altra, tra *sviluppo* (*della disciplina e delle sue applicazioni*) e *manutenzione correttiva, adattiva e evolutiva.* Tale rilevante distinzione, di grande utilità anche dal punto di vista espositivo, ha l'obiettivo di guidare gli addetti ai lavori e non solo verso la predisposizione di «un *ambiente idoneo* allo sviluppo di una informatica medica rispettosa dei principi e della legislazione di ciascuno Stato in cui opera» (p. 25).

A conclusione del primo capitolo – secondo un modulo tale per cui ogni capitolo termina con un focus dedicato a tematiche centrali dell'informatica medica – alcune pagine sono dedicate all'infermieristica informatica (pp. 38-40), settore specifico dell'informatica medica che ha subito nel corso degli ultimi due decenni diversi cambiamenti per via dell'implementazione di nuove tecnologie e di sistemi informatici sempre più avanzati. Tanto da un punto di vista teorico che pratico, la figura dell'infermiere ha assistito ad un adeguamento dei suoi compiti professionali ai molteplici utilizzi delle tecnologie informatiche. Si pensi, per esempio, alla raccolta, alla conservazione e alla contestuale analisi dei dati dei pazienti o alla consultazione, mediante supporti informatici, di informazioni utili a supportare e migliorare la cura dell'assistito.

Il secondo capitolo prende in considerazione diversi argomenti cardine dell'informatica giuridica e, sempre sotto la lente dell'informatica medica, ne sottolinea alcuni profili etici e giuridici meritevoli di essere approfonditi.

In particolare, Fioriglio si concentra sul tema dell'intelligenza artificiale partendo da alcuni essenziali cenni storici per arrivare a spiegare l'interessante relazione che quest'ultima intrattiene con l'informatica medica e i campi d'applicazione che la vedono protagonista. Per affinità tematica, nelle stesse pagine l'Autore fa menzione della medicina algoritmica, sottolineando che il suo ruolo è ancora del tutto ancillare rispetto alla medicina tradizionale a causa delle numerose problematiche e di alcune perplessità che la interessano (pp. 41-55).

In seguito, l'attenzione viene spostata sul diritto alla privacy e sulla protezione dei dati personali, elementi costanti nel settore della salute e nell'informatica medica. L'Autore sottolinea come spesso il raggiungimento di determinati successi in campo tecnologico e, più in particolare, informatico non sia sempre accompagnato dal rispetto della dignità e della privacy della persona, quasi come se si stesse parlando di diritti più che occasionalmente sacrificabili. A questo proposito, anche grazie all'attento esame del Regolamento generale sulla protezione dei dati (Regolamento UE, n. 2016/679), si sostiene che il diritto possa essere a tutti gli effetti uno strumento efficace nello sviluppo tecnologico in ambito medico «non quale limitazione, bensì quale stimolo e controllo per farlo procedere senza violare la dignità e la privacy della persona» (p. 65).

L'Autore si interroga poi sulla vasta quantità di informazioni a carattere medico, o presunte tali, presenti in rete e si esprime sulla decisiva importanza della loro correttezza soprattutto laddove la mancanza di quest'ultima potrebbe avere conseguenze negative dirette su tutti coloro che ne usufruiscono (pp. 65-72). Infatti, in campo medico, l'accessibilità diffusa a informazioni sanitarie di carattere generale e specifico garantita dalla rete Internet non può che essere un grande beneficio per il cittadino digitale del terzo millennio. A patto, però, che si possa fare affidamento su fonti attendibili. In caso contrario,

trattandosi di informazioni che possono influenzare il giudizio di una persona in merito a tematiche indubbiamente serie come quelle relative alla salute, la scarsa qualità o addirittura l'erroneità di tali informazioni potrebbero comportare rischi più o meno gravi per la salute dell'individuo.

Attraverso la definizione di due requisiti, uno obbligatorio e uno raccomandato, si auspica che il diritto possa giocare un ruolo fondamentale nel garantire che ogni utente possa contare su informazioni inerenti alla salute che siano corrette e affidabili.

La chiusura del capitolo è dedicata al tema dei "Big Data", evidenziando come questa "riduzione della realtà" (p. 74) possa condurre a problemi tanto di carattere etico quanto giuridico. In particolare, si osserva come l'acquisizione informatica di grandissimi quantitativi di dati, come in questo caso, sia spesso accompagnata da lesioni del diritto alla privacy e alla protezione dei dati personali. In molti casi, infatti, la tutela di tali diritti viene considerata più come un ostacolo che non come un'opportunità di rispettare compiutamente l'identità e la dignità dei soggetti interessati. Successivamente, vengono presi in considerazione sia la possibile presenza di *bias* nella formulazione degli algoritmi sia l'abituale imperscrutabilità degli strumenti tecnologici (es. software) che vengono utilizzati per la raccolta dei Big Data. La necessità di non ignorare tali problematiche si fa sicuramente più impellente se le si considera alla luce dell'informatica medica e del comparto di diritti che la riguardano, primi fra tutti il diritto alla vita e quello alla salute.

Infine, il terzo capitolo è dedicato interamente alle applicazioni e alle prospettive specifiche dell'informatica medica. Per prima cosa, vengono analizzati i sistemi informativi sanitari, la cui corretta implementazione può portare a un netto miglioramento dell'assistenza sanitaria. Successivamente, l'Autore illustra l'esempio degli *Electronic Health Records*, o "cartella clinica elettronica", uno strumento di grande rilevanza che permette di raccogliere in un unico spazio elettronico una serie di informazioni principalmente sanitarie relative a un determinato paziente. A questo proposito, Fioriglio si interroga sulla mancanza di standard informatici comuni che permettano ai vari dispositivi che raccolgono o conservano tali informazioni di comunicare efficacemente tra loro e suggerisce, quindi, che la previsione di uno standard generalizzato sia il prossimo passo da compiere per adeguarsi ad una società sempre più globalizzata.

Le ulteriori aree di applicazione che vengono di seguito trattate sono quelle relative alla robotica e al potenziamento umano, per poi passare in rassegna alcuni aspetti specifici della telemedicina e della *mobile health* (*mHealth*) e concludere con la trattazione della medicina personalizzata e la medicina di precisione, entrambe da considerarsi come evoluzioni della medicina moderna (pp. 84-99).

Il focus di questo capitolo è dedicato al Fascicolo Sanitario Elettronico (FSE) e all'insieme di norme che ne regolano il funzionamento e, soprattutto, garantiscono la tutela dei diritti di privacy e protezione dei dati personali. Si tratta di aspetti che stanno mostrando tutto il loro impatto nel contesto pandemico.

L'opera di Fioriglio, dunque, consente di approfondire la materia dell'informatica medica sottolineandone l'intenso rapporto che intercorre tra quest'ultima e il diritto. L'Autore ribadisce più volte come la stessa informatica medica non possa fare a meno dell'ausilio che il diritto può fornirle per evolversi in senso pieno. Infatti, solo il rispetto dei principi e dei valori costituzionali interessati dalle differenti applicazioni dell'informatica in ambito medico possono far sì che diritti fondamentali come quello alla vita e quello alla salute siano garantiti e tutelati per tutti e tutte.

A partire dalla piena consapevolezza che le tecnologie informatiche incidono profondamente sull'evoluzione della scienza medica, l'opera – frutto di una ricerca ormai ventennale – argomenta come il diritto non possa permettersi di rimanere ai margini.

Esistono le condizioni affinché ciò possa essere di fatto scongiurato e affinché le tecnologie possano essere sviluppate mantenendo al primo posto la dignità e la salute di ogni individuo.