RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

2•2023

SEZIONE MONOGRAFICA

La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale

a cura di Simone Calzolaio
con la collaborazione di Federico Serini

CONTRIBUTI DI

S. Calzolaio • A. Cossiri
E. Cremona • A. Di Corinto
C. Lobascio • E. Longo • F. Serini
I. Sigismondi • S. Torregiani

diretta da **Sebastiano Faro • Marina Pietrangelo**

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

anno V • periodicità semestrale • ISSN 2704-7318

www.rivistaitalianadiinformaticaediritto.it

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto

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

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

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

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

Nel corso della sua storia la Rivista è stata accompagnata, e continua ad esserlo, da un prestigioso gruppo di corrispondenti stranieri: Y. Amoroso *CUB*, T.J.M. Bench Capon *GBR*, D. Bourcier *FRA*, W.E. Boyd *USA*, V. De Mulder *NLD*, J. Dumortier *NLD*, F. Galindo *ESP*, A. Gardner *USA*, T. Gordon *DEU*, G. Greenleaf *AUS*, O.P. Hance *LUX*, W. Kilian *DEU*, F. Lachmayer *AUT*, P. Leith *IRL*, E. Mackaay *CAN*, A. Maclntosh *GBR*, P. Maharg *GBR*, J. Mayor *USA*, L.T. McCarty *USA*, F. Novak *CZE*, A. Paliwala *GBR*, A.E. Perez-Luño *ESP*, R. Petrauskas *LTU*, L. Philipps *DEU*, Y. Poullet *BEL*, A. Saarempaa *FIN*, E. Schweighofer *AUT*, P. Seipel *SWE*, R. Susskind *GBR*, W.R. Svoboda *AUT*, H. Yoshino *JPN*, T. Van Engers *NLD*, M.A. Wimmer *AUT*, R. Winkels *NLD*, J. Zeleznikow *AUS*.

Segretaria di redazione Simona Binazzi
Elaborazione testi e grafica Giuseppina Sabato
Responsabile del sito web Elisabetta Marinai

Direzione e Redazione
IGSG/CNR • Via dei Barucci, 20 • 50127 Firenze
Tel. +39 055 43995 • rivistaRIID@igsg.cnr.it • www.rivistaitalianadiinformaticaediritto.it

Direttore responsabile
Sebastiano Faro • Registrazione presso il Tribunale di Roma al n. 127/2019

2·2023

Indice

Sezione monografica

La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale

a cura di Simone Calzolaio con la collaborazione di Federico Serini

Studi e ricerche

Note e discussioni

Osservatori

Recensioni

Sezione monografica

La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale

a cura di

Simone Calzolaio

con la collaborazione di Federico Serini

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0133 • articolo non sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Simone Calzolaio

La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale
Introduzione

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

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Che cosa resta dell'utopia di Internet? La rete Internet doveva renderci più liberi, più informati e più consapevoli, più uniti in un unico piccolo mondo, più tutelati e più sicuri rispetto agli altri umani, ai poteri pubblici e ai poteri privati. La rete Internet doveva essere il nuovo stadio e forse anche l'ulteriore inedito lascito delle liberaldemocrazie al mondo. Le cose stanno andando – come per tutte le utopie – molto diversamente. L'avvento e l'evoluzione della rete Internet sono ormai divenute il terreno di una nuova era della regolazione giuridica: l'esigenza di governo della sfuggente società dei dati. Proviamo, in questa sezione monografica della *Rivista italiana di informatica e diritto*, a passare in rassegna – con la piena consapevolezza che la materia di studio è più grande delle capacità di ciascuno – quali sono alcuni dei nuovi ambiti e dei nuovi strumenti di questa sfida regolatoria, da una prospettiva schiettamente liberaldemocratica.

2. La sezione trae spunto dal convegno ICON•S di Bologna su *Il Futuro dello Stato*[1] e dal panel che si è avuto l'opportunità di co-organizzare[2] in tale sede.

Nell'ambito della tematica del *Futuro dello Stato* ci era sembrato interessante porsi il problema – provocatoriamente – della fine della rete Internet così come l'avevamo conosciuta e delle sfide pressanti che l'avvento della società digitale comportava per la democrazia. Il titolo del panel era *La fine di Internet? vulnerabilità della democrazia e regolazione delle piattaforme*, mentre il titolo di questa pubblicazione collettanea non è più esclusivamente rivolto alla regolazione delle piattaforme, ma più ampiamente alle sfide della regolazione e gestione dello spazio digitale.

In effetti, la situazione e la condizione post-pandemica, insieme ai venti di guerra che avvolgono direttamente l'Europa, hanno manifestato l'esigenza di indagare sfide e piste meno battute di quelle della regolazione dei *bad guys* delle *big tech*. I contributi di questa sezione monografica rappresentano esattamente questa nuova dimensione.

3. Il primo aspetto di cui si avverte l'esigenza – a nostro sommesso avviso – è un quadro realistico delle vulnerabilità caratteristiche della società digitale e quindi indotte, specificamente, dal (mutevole) processo di datificazione. Proprio dall'indagine delle vulnerabilità si rendono manifeste le domande aperte ed i profili di tutela costituzionale a maggior rischio: la prima vulnerabilità della società digitale può consistere nella difficoltà ad identificare i caratteri specifici di un ordinamento dei dati (su questo aspetto si avventura il contributo *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*).

Si è ritenuto opportuno – grazie al lavoro di Camilla Lobascio – mettere a disposizione del lettore una tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme, che senza pretesa di esaustività, al fine di agevolare lo studio e il reperimento di materiali normativi, elenca le principali disposizioni del diritto europeo dei dati e delle piattaforme digitali, vigente o ancora in fase di discussione, con specifico link al sito ufficiale dell'Unione europea, ove è possibile approfondire i lavori preparatori e reperire altro materiale ufficiale.

Un secondo aspetto – che emerse proprio grazie ad un puntuale intervento svolto oralmente da Federico Serini in occasione del panel e che contribuì a modificarne l'oggetto, così come descritto – concerne l'urgenza di qualificare e descrivere la più recente delle grandi vulnerabilità delle nostre democrazie: la dimensione della sicurezza cibernetica, in tutte le sue consistenti sfaccettature. Appare davvero meritorio il tentativo di Serini di spiegare, e con ciò legare, i modelli di sicurezza cibernetica al rilievo normativo assunto dalle pratiche di standardizzazione delle norme tecniche, e dei connessi modelli di certificazione, che di fatto rappresentano le vere e uniche regole cogenti della società digitale.

Il contributo di Angela Cossiri ci introduce al rilievo delle c.d. campagne di disinformazione ed alla vulnerabilità dei tessuti democratici – si direbbe dovuta proprio al fatto di essere tali – di fronte a queste vecchie armi della propaganda, sviluppate con gli strumenti tipici della società digitale. Si descrivono il fondamento e la dinamica della Decisione Pesc 2022/351 del Consiglio, peraltro non così chiaramente

1. V. il sito del Convegno ICONS•S.
2. … sempre grazie alla cordialità degli organizzatori di ICON•S e alla vivacità intellettuale di colleghe e colleghi: v. il programma del Convegno.

approfonditi finché non vennero esposti da Angela Cossiri durante il panel bolognese, riguardante le modalità con cui l'Unione europea si è difesa – adottando azioni e prassi istituzionali anch'esse sostanzialmente inedite – di fronte all'attacco informativo subito in concomitanza all'avvio della guerra russo-ucraina e ai suoi sviluppi in sede giurisdizionale, ove con motivazione interessante il provvedimento europeo è stato ritenuto legittimo.

Nel contributo di Arturo Di Corinto si descrivono le dinamiche e l'articolazione della vera e propria guerra cibernetica, che si sviluppa nel campo di battaglia della Rete, fiancheggiando le attività degli eserciti sul campo, per sostenere gli obiettivi strategici della propria parte e fiaccare le resistenze degli avversari: è l'infowar con i suoi soldati, gli hacktivisti. Il campo di battaglia – e di indagine – purtroppo è lo scenario del conflitto russo-ucraino.

Lasciando da parte le guerre vere e proprie, il contributo di Irene Sigismondi si occupa invece di descrivere come si possano evitare – grazie alla Rete – le guerre giudiziarie nelle aule di tribunale, per trasferirle nell'ambiente digitale della rete Internet, in particolare attraverso l'utilizzo delle online dispute resolution (ODR), ovvero delle piattaforme di risoluzione alternativa delle controversie: non è affatto irrilevante, e ci mostra come la fine dell'utopia di Internet investa proprio gli aspetti che ne rappresentavano l'iniziale ed intrinseco contenuto originario, che uno degli aspetti che mette a rischio l'utilizzo e lo sviluppo delle ODR, sia proprio la progressiva frammentazione della rete Internet.

Gli ultimi due contributi aprono il quadro di indagine agli sviluppi normativi più recenti ed alle dinamiche di cui si avverte maggiormente l'esigenza per consentire uno sviluppo pieno e sovrano della dimensione europea della società digitale. Elia Cremona espone chiaramente la sua tesi, secondo cui il Data Governance Act e il Data Act costituiscono un mutamento di paradigma dell'indirizzo normativo europeo: l'enfasi non è più solo sul profilo della protezione e del controllo, ma anche della condivisione. La parola d'ordine è il data sharing e gli strumenti sono – principalmente – l'intermediazione, l'altruismo, l'accessibilità. Il fine è riconoscere che i dati sono beni comuni del nostro tempo: la loro condivisione, specie dal settore privato a quello pubblico, può rappresentare un'opportunità per lo sviluppo di politiche pubbliche data-driven e, per le imprese, di contribuire al raggiungimento degli obiettivi di sostenibilità fissati dalla normativa ESG (Environmental, Social, Governance).

Stefano Torregiani si pone il problema dell'impatto della datificazione sulla sovranità dell'Unione europea e osserva – obiettivamente, a ragione – che dei dati europei non hanno beneficiato principalmente i cittadini europei. Si chiede quindi se il recente Data Act – con l'obiettivo dichiarato di consentire accesso e riuso dei dati – possa riportare l'Unione in una dimensione di maggior padronanza e sfruttamento delle sue risorse digitali: è forse il Data Act una forma di Data Nationalism europeo? E in tal caso, può rivelarsi una strategia efficace?

4. La pluralità e i differenti punti di vista dei contributi raccolti rendono necessaria una ritrovata visione unitaria, ma non asfittica, della dimensione costituzionale della società digitale: concludendo e commentando i lavori di questa sezione monografica Erik Longo mostra che riconoscere il data-centrismo non implica aderire ad una ideologia – ottimista o pessimista – dei dati e della loro funzione. Implica invece riconoscere nel nuovo contesto tecnologico e nei mutamenti antropologici in atto l'esigenza di porre la tecnologia a servizio delle esigenze umane di giustizia (giustizia dei dati), di conoscibilità e spiegabilità (trasparenza algoritmica) e di controllo della tecnologia (controllo umano).

This research was funded by the European Union – NextGenerationEU under the Italian Ministry of University and Research (MIUR), National Innovation Ecosystem grant ECS00000041-VITALITY-CUP D83C22000710005

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0131 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Simone Calzolaio

Vulnerabilità della società digitale e ordinamento costituzionale dei dati

La fine delle prospettive utopiche connesse all'avvento della rete Internet ha lasciato sul campo molteplici esigenze di regolazione, che si colgono osservando empiricamente le vulnerabilità che caratterizzano la persona ed il sistema democratico nella società digitale. In tale contesto, uno degli aspetti che rende più fragile e rischiosamente frammentato l'ordinamento giuridico di fronte alla evoluzione digitale consiste nella difficoltà di individuare in modo sistematico i caratteri emergenti del processo di datificazione. In questo contributo si tenta di identificare alcune caratteristiche ricorrenti dell'ordinamento dei dati e di verificare la possibilità, nell'ambito del sistema costituzionale dei valori e delle libertà, di continuare a garantire il primato della tutela della persona umana e del contesto sociale in cui si svolge la sua personalità, pur di fronte a nuove sfide epocali.

Internet – Ordinamento costituzionale – Ordinamento dei dati – Dati sintetici – Connessione sociale

The digital society vulnerabilities and constitutional data legal system

The end of the utopian perspectives connected to the advent of the Internet has left multiple needs in the field of regulation, which are captured by empirically observing the vulnerabilities that characterize the person and the democracy system in the digital society. Faced with digital evolution, the legal system needs to identify a legal data system that clarifies the characteristics of datafication and avoids the danger of legal fragmentation. In this contribution we attempt to identify some recurring characteristics of data system and to verify the possibility, within the constitutional system of values and freedoms, to continue to guarantee the primacy of the protection of the human person and the social context in which his personality unfolds, despite facing new epochal challenges.

Internet – Constitutional law – Data law – Synthetic data - Social connection

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

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

"Addio", disse la volpe. "Ecco il mio segreto.
È molto semplice: non si vede bene che col cuore. L'essenziale è invisibile agli occhi".
"L'essenziale è invisibile agli occhi", ripeté il piccolo principe, per ricordarselo.
"È il tempo che tu hai perduto per la tua rosa che ha fatto la tua rosa così importante".

(Antoine de Saint-Exupéry, Il piccolo principe)

1. Oggetto del contributo

Scopo di questo lavoro – che prende spunto dal convegno ICON•S di Bologna su *Il Futuro dello Stato*[1] e dal panel che si è avuto l'opportunità di co-organizzare[2] – è contribuire a:

1) descrivere le vulnerabilità che l'avvento della società digitale sta mostrando in pressoché tutti gli ordinamenti costituzionali liberaldemocratici;
2) individuare alcuni punti fermi che l'analisi giuridica della società digitale, come società dei dati, evidenzia e che sono aspetti nodali per qualunque costruzione giuridica e regolatoria: si tratta dei primi aspetti di un ordinamento costituzionale dei dati (non più solo dei dati personali);
3) provare a identificare spunti di approfondimento che si scorgono come più pressanti all'orizzonte e che mettono alla prova la *vitalità* della nostra Costituzione e dell'ordinamento costituzionale italiano[3] ed europeo su aspetti classici del costituzionalismo liberaldemocratico.

2. Dall'utopia alle vulnerabilità: l'esigenza di un ordinamento costituzionale dei dati

Poco dopo la caduta del muro di Berlino e la sofferta – ma pacifica – conclusione della grande utopia del socialismo reale del secondo Novecento, v'era un clima euforico[4] nel mondo occidentale e nel rinato mondo orientale. Proprio agli albori di quella che si sarebbe chiamata "globalizzazione" faceva il suo ingresso nella storia una nuova rete: "Internet", nata per garantire le comunicazioni nel caso in cui la guerra fredda si fosse improvvisamente surriscaldata, finiva per venire divulgata

1. V. il sito del Convegno ICONS•S.
2. … sempre grazie alla cordialità degli organizzatori di ICON•S e alla vivacità intellettuale di colleghe e colleghi: v. il programma del Convegno.
3. Per ordinamento costituzionale intendiamo – come si vedrà – quanto autorevolmente individuato da Barbera 2010.
4. Si veda ancora oggi, ad esempio, Ash 2023, il quale descrive il periodo 1990-2007 della storia europea con il significativo titolo "Il trionfo". Qualcuno era meno utopico degli altri, qualcuno aveva intuito che il crollo del muro di Berlino avrebbe indotto, in Italia in particolare, altri crolli: cfr. Cossiga-Chessa 2007.

in tempo di pace come strumento di connessione mondiale, di collaborazione, di partecipazione da una parte all'altra del globo, da ovest ad est[5].

Un ottimismo utopico ha accolto l'avvento di Internet[6]: un ulteriore lascito della democrazia americana, che sembrava destinata a far crollare l'uno dopo l'altro tutti i muri che separavano gli esseri umani: libertà dell'est Europa (e dalla paura di una guerra nucleare), libertà dei commerci mondiali e con l'est del mondo, libertà di comunicazione e di informazione globale senza (possibilità di) censure, senza costi, per tutti.

Non tutti lo ricordano, ma alla base della tuttora vigente regola statunitense sulla responsabilità degli Internet service provider[7] – una regola materialmente costituzionale – vi era esattamente questo sentimento di ineluttabilità delle magnifiche sorti e progressive dell'umanità, che grazie al libero sviluppo di questa nuova tecnologia, e alla libera intelligenza collettiva che ne scaturiva, avrebbe trovato – attraverso la regia/supremazia americana[8] – progressivamente soluzione a tutti i suoi problemi.

In principio era Internet e lo immaginavamo diverso[9], in sintesi.

In quella prima fase, a farne le spese in ambito giuridico, furono principalmente il diritto della proprietà intellettuale, il diritto d'autore e la protezione dei dati personali.

Poi la Rete si è evoluta: l'avvento della banda larga, con lo sviluppo dei connessi servizi digitali, il web 2.0 interattivo, i servizi di messaggistica istantanea, l'i-phone e poi gli smartphone, i social media, la digitalizzazione pubblica, i motori – e poi, il motore – di ricerca e le piattaforme digitali, l'IOT, il cloud computing. Infine, quell'oggetto ancora largamente inesplorato e ignoto che chiamiamo convenzionalmente intelligenza artificiale.

Nel corso dell'ultimo decennio, accanto al progresso fulminante abbiamo cominciato a scorgere gli effetti, le incognite, i mutamenti indotti dalla evoluzione tecnologica (Pasquale, Cohen, Zuboff). L'ottimismo si è mutato in un più semplice arrendersi al dinamismo indotto dall'inesauribile sviluppo tecnologico. Distolto lo sguardo dal sole accecante dell'utopia, si intravedono ora i rischi (i danni, talvolta), le nuove divisioni sociali e geopolitiche, il ritorno di antichi poteri[10] per affrontare le vulnerabilità delle società (digitali)

5. Cfr. Elmer-Dewitt 1993; v. più di recente Amenta 2015.
6. … che doveva essere uno spazio statuale libero e libertario: «We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before», così Barlow 1996.
7. Come osserva Finocchiaro 2022, p. 815: «Gli Stati Uniti con il Communications Decency Act del 1996 [n.d.a., sez. 230: "Nessun provider o utente di un servizio informatico interattivo deve essere trattato come editore o creatore di qualsiasi informazione fornita da un altro provider di contenuti informativi"] e poi l'Europa con la Direttiva 2000/31/CE sul commercio elettronico statuirono una sostanziale esenzione di responsabilità del provider. Si era in un'epoca completamente diversa: eravamo all'inizio della diffusione del web e quindi occorreva lasciare che la comunicazione digitale seguisse il suo corso espansivo, senza onerarla di costi che inevitabilmente sarebbero stati riversati sugli utenti. Naturalmente questa è solo una delle prospettive di lettura – se ne potrebbero aggiungere molte altre – ma è probabilmente quella più accreditata dal punto di vista funzionale ed economico». V. anche Riccio 2002, p. 171 ss., in merito al DMCA (*Digital Millenium Copyright Act*) e al OCILLA (*Online Copyright Infringement Liability Limitation Act*).
8. … altra più recente grande disciplina – questa sì, materialmente costituzionale e intrinsecamente volta a rivendicare una forma di supremazia globale – è il CLOUD Act statunitense (acronimo che sta per *Clarifying Lawful Overseas Use of Data Act*), su cui, davvero interessante: Boncinelli 2021, spec. p. 36 ss.
9. Così Scorza 2022, p. 23 ss.
10. Davvero interessante: Morrone 2023, il quale giustamente si domanda – come pure faremo qui naturalmente – «La domanda vera, allora, non riguarda il "ritorno dello Stato" ma è: "quale Stato ritorna oggi?"» (p. 270) e poi sviluppa, anche in riferimento al governo del digitale, la tesi e l'auspicio della ri-politicizzazione dello Stato.

contemporanee[11]: «nessuno crede più alla retorica dello spazio digitale come luogo della libertà»[12].

Sta di fatto che ormai assistiamo al blocco sistematico e ricorrente, da parte di Stati (di norma autoritari), della rete Internet per evitare le comunicazioni e l'informazione delle persone in vista di avvenimenti importanti o di rilievo sociale[13] o per sedare rivolte o per placare gli animi social: l'ultimo caso è quello delle elezioni pakistane[14], ma altrettanto avviene in Israele e in Palestina, e in molte altre parti del mondo. Lo Stato, il potere nega internet alla sua gente[15] per affermare la sua supremazia (spesso autoritaria).

Ma altrettanto spesso, in diverse aree del mondo, quando lo Stato non nega (all'interno dei suoi confini) la Rete è perché si tratta di uno strumento inarrivabile per misurare, controllare, sorvegliare le persone: è il caso del *social scoring* cinese[16]. Che non è così isolato e lontano come vorremmo credere[17], ad esempio nel caso dell'ormai diffuso *credit scoring*[18]. Basta fare esperienza dei software di registro elettronico in uso presso le scuole pubbliche, per capire come sotto le specie della "trasparenza informativa" e della collaborazione scuola-famiglia, la dimensione digitale insinui quasi spontaneamente una forma pervasiva di "sorveglianza", e come questi modelli rischino di schiacciare i più deboli fra gli studenti (e fra i professori), in una apparente oggettivizzazione e, appunto, datificazione (intesa come riduzione alle informazioni che derivano dai dati) della vita scolastica. Eppure, anche questa è la rete Internet e non v'è nulla di più popolare fra genitori (ansiogeni) e professori (intimoriti e distanti) del controllo sistematico e immediato dei propri figli e studenti da remoto: liberi, ma mai di agire inosservati. Cioè: sorvegliati.

Ma pensiamo ancora alle capacità dei *Large Language Models* (LLM), all'intelligenza artificiale cd. generativa, che apprendono dalla rete (*web-scraping*[19] e altre modalità) e da altri data set e sono in grado di scrivere questo articolo[20] in

11. Questo rovesciamento dell'utopia, si sostanzia nella ritenuta progressiva frammentazione della rete Internet, in una molteplicità di reti nazionali e sovranazionali, in zone di influenza geopolitica, in piccoli spazi privati: cfr. Lemley 2021.
12. Bergonzini 2023, p. 99.
13. L'Internet society monitora il blocco di Internet nelle varie nazioni del mondo e le sue motivazioni. È una strana cartina geografica del mondo, che vale la pena osservare.
14. Cfr. Zorloni 2024.
15. Cfr. De Gregorio-Stremlau 2020, i quali ragionevolmente osservano: «we do not deny that Internet shutdowns constitute a highly intrusive form of censorship, there are reasons when these practices could be justified. This is not, in any way, to endorse or condone such actions, but we argue that in the context of a rising tide of incitement to violence on social media platforms (and an apparent inability of social media actors to curb such speech) there needs to be a more nuanced and transparent conversation about why some governments are taking the seemingly extreme actions they are, how they can be limited, or when they might be justified, and how concerns about widespread hate online can be better brought into debates around the protection of human rights».
16. Cfr. Cheung-Chen 2022; sul tema più generale del riconoscimento facciale, v. Mobilio 2021.
17. Cfr. Citino 2023, la quale riporta il famoso caso olandese Syri, ma altresì casi di *social scoring* sviluppati da istituzioni territoriali: non sono sempre e solo gli Stati ad adottare politiche di tal fatta, che peraltro in alcuni casi potrebbero perfino essere ragionevoli e utili, o comunque motivabili adeguatamente.
18. Si veda la recentissima CGUE, sentenza 7 dicembre 2023 in C-634/21, secondo cui l'attività di *credit scoring* può costituire un "processo decisionale automatizzato" ai sensi del GDPR laddove da tale punteggio dipenda, in modo decisivo, la stipula, l'esecuzione o la cessazione di un rapporto contrattuale tra l'interessato ed il soggetto terzo al quale è comunicato il predetto *score* probabilistico.
19. Cfr. Lobel 2021, spec. p. 185 ss.
20. Lo aveva capito prima, perché l'intelligenza è innanzitutto un dono, Caravita 2020, p. 470, par. 8, intitolato proprio "Questo testo non è stato scritto da una macchina di intelligenza artificiale, ma un domani…?". Quel domani è arrivato presto.

modo più puntuale, specifico, brillante, dotto, e soprattutto veloce e senza costi, di un misero e costoso essere umano, riproducendo tuttavia la visione, il modo di scrivere e di *interpretare* insito nelle modalità di apprendimento del sistema (è il caso *New York Times vs. ChatGpt*[21]), che altro non è poi che la vecchia tirannia della maggioranza (istituzionalizzata, in questo caso, dal design della tecnologia), di cui parlava un francese in viaggio negli States[22]. In genere, quando si ricorre a questo esempio la mente scorre verso il problema della sostituzione delle macchine ai colletti bianchi, ai professionisti, ai professori, ai giudici, ai medici, oltre che dei robot agli operai ed agli agricoltori. In realtà, è opportuno domandarsi[23]: quali capacità stiamo perdendo se non siamo più costretti a scrivere, ad apprendere questa o quella abilità seguendo una disciplina, e spesso qualcuno che ce la insegni, poiché c'è chi lo fa per noi, e meglio di noi, senza di noi? Come distingueremo un volto umano da un volto umano sintetico? Non si tratta di essere romantici, ma di affrontare il tema della libera formazione della personalità e, quindi, della libertà di formazione del pensiero[24] dopo l'avvento della società digitale.

Infine: la rete Internet, i suoi fantastici servizi gratuiti, le auto e le bici connesse con gli smartphone connessi con la domotica connessa e con gli acquisti online e il cibo a casa, con un bel libro digitale e la tv-online. Il problema della *iper-connessione* e della sua incidenza sulle relazioni sociali, sulla formazione dei minori, sulla edificazione del sistema dell'informazione e infine sulla impercettibile ma costante perdita di libertà cognitiva attraverso l'ineluttabile *engagement* con questo o quel social, app, game, di cui – solo per oggi – non possiamo fare a meno. Ormai la vita è digitale, senza una vera cittadinanza digitale[25], e con molte invisibili nuove forme di dipendenza, compresa la difficoltà pratica ed emotiva di disconnettersi dal lavoro[26].

Tutto questo significa che siamo perduti? No.

Il progresso indotto dalla società digitale è evidente e lo si potrebbe descrivere ancor più analiticamente di quanto non si siano – senza possibilità di essere esaustivi – descritte le vulnerabilità più marcate.

Peraltro, si sono tralasciati i temi posti dalle *big tech* private, dalle piattaforme digitali e l'altro grande tema delle libertà politiche e dei processi democratici, ma solo perché sono vicine alla tradizionale sensibilità costituzionalistica e già approfonditamente considerate[27].

Si è trattato però di lasciare sin qui emergere un po' brutalmente l'evidenza che l'utopia di Internet è ormai un ricordo e, ora, è necessario fare i conti con la datificazione e con le esigenze di governo dei dati, da cui dipende largamente la sopravvivenza e l'evoluzione del tessuto costituzionale e, con esso, delle democrazie[28].

Cerchiamo quindi di procedere ad individuare i caratteri di base dell'ordinamento costituzionale

21. Qui un atto giuridico di sicuro rilievo, l'atto di citazione del NYT a GPT e Microsoft. Ma l'aspetto interessante è che le modalità di addestramento della LLM non possono che tendere a rappresentare e riprodurre la mentalità – il capitale semantico, direbbe forse Floridi, cfr. Floridi 2018 – derivante dai dati con cui il LLM è addestrato: per intenderci, se i dati derivano dal principale quotidiano newyorkese, principalmente WASP. Pertanto, il rischio che la LLM diventi uno strumento di influenza culturale subliminale è reale, anche se gli studi più recenti di Microsoft ci dicono: a) che la IA generativa funziona meglio con "piccoli dati", cioè dati settoriali di qualità, come i classici manuali: cfr. Gunasekar et al. 2023; b) che la IA generativa può essere addestrata a dimenticare, a disapprendere quanto appreso, e quindi l'addestramento può diluire i pregiudizi di mentalità, gli eventuali danni generati, e può rispettare la proprietà intellettuale: cfr. Eldan-Russinovich 2023.
22. De Tocqueville 2005.
23. Freuler 2023.
24. Indispensabile la lettura di Richards 2015, e volendo Calzolaio 2018, pp. 366-369.
25. Ma v. su questo Costantino 2023.
26. Cuomo 2023.
27. Cfr., rispettivamente, Bergonzini 2023, Caruso 2023, Di Cosimo 2023, Manetti 2023.
28. Cfr. Manetti 2020.

dei dati[29] – procedendo nell'indagine si darà ragione dell'utilizzo dei tre termini (ordinamento, costituzionale, dati) –.

3. Alcuni punti fermi: dalla *data driven innovation* alla *data dependency*

In piena pandemia[30] fu semplice accorgersi del fatto che si era realizzato un passaggio netto in quegli anni: l'ottimismo intrinseco nell'idea retorica dell'intelligenza collettiva di Internet aveva una propaggine rilevante nella dimensione concettuale della *data-driven innovation*[31]. Tuttavia, quella fase è superata: ormai la dimensione di raccolta, disponibilità, sfruttamento, messa a disposizione, condivisione dei dati è coessenziale per garantire la vita ordinaria delle società contemporanee. L'innovazione passa per lo sfruttamento dei dati perché dipendiamo dai dati in tutti gli aspetti della nostra vita (compresa l'innovazione tecnologica).

Tre esempi. Abbiamo accennato alle ipotesi di *Internet shutdown*. Possiamo chiederci: come avrebbero agito gli stessi poteri pubblici che hanno bloccato Internet, 30 anni fa? Avrebbero censurato la radiotv e la stampa, vietato le manifestazioni, represso il dissenso con la forza. Può darsi lo facciano anche ora – ma è più semplice rimuovere la leva che aggrega e motiva le persone: bloccare Internet, bloccare la comunicazione, bloccare la diffusione di notizie, cioè bloccare la circolazione dei dati in particolare attraverso i social media, incide sulle modalità ordinarie con cui le persone ormai comunicano fra loro e acquisiscono informazioni e notizie. Le persone dipendono dalla circolazione dei dati e delle informazioni attraverso la Rete e i social media. Si tratta di una questione di diritto costituzionale.

Il Governo Conte I, con una certa disinvoltura (ma non isolatamente a livello europeo), stava concretamente vagliando, per il tramite di un membro del Governo vicino al governo cinese, la possibilità di affidare la costituzione della rete 5G a un noto operatore cinese[32]. In via ufficiale, l'ambasciata statunitense affermò che la Nato e gli Stati Uniti avrebbero, in tal caso, limitato la condivisione di informazioni con l'Italia[33]. Pochi mesi più tardi la vicenda assunse tutt'altra piega[34] e, come noto, poi l'esperienza di quel governo si concluse (il 4 settembre 2019). Le infrastrutture materiali e immateriali attinenti alla circolazione dei dati rappresentano una questione dirimente di interesse e sicurezza nazionale e di collocazione geopolitica. Gli Stati dipendono dalla circolazione dei dati e delle informazioni attraverso la rete Internet e dalle relative infrastrutture. Si tratta di una questione di diritto costituzionale[35].

Immaginiamo di privare un adolescente infratredicenne della possibilità di frequentare la sua comunità di pari con gli strumenti digitali che questa (lecitamente) utilizza: messagistica istantanea, social media, giochi online, Internet tv, ecc. Questo adolescente, di norma, avvertirà un senso percepibile di esclusione e di segregazione, molto simile a quello di un adolescente che fino agli anni Duemila fosse stato impedito stabilmente di frequentare personalmente la stessa comunità di suoi pari. La formazione della personalità passa attraverso gli strumenti che la contemporaneità offre e fra questi – seppure, come vedremo, rischiosissimi – ci sono gli strumenti digitali: un adolescente di oggi che ne fosse (totalmente e permanentemente) escluso, ne sarebbe menomato. Ma questo, se ci osserviamo un istante, vale per tutti noi.

29. Vi è una connessione fra l'identificazione di questi caratteri dell'ordinamento dei dati e la qualificazione privatistica della titolarità dei dati: cfr. Marinotti 2022.
30. Si veda Calzolaio 2021a.
31. Si veda a questo riguardo la descrizione di questo aspetto, volendo, in Calzolaio 2017, spec. p. 602, con relativi riferimenti.
32. Cfr. Bechis-Mieli 2019.
33. Cfr. Pierri 2019.
34. … con l'adozione di indirizzi governativi che di fatto rendevano impossibile la partecipazione delle aziende cinesi: cfr. Arnese-Walsingham 2020; ora il Piano Italia 5G è confluito nel PNRR, ma non sembra stia avanzando con sufficiente rapidità.
35. Su questo aspetto, v. Salerno 2018, spec. p. 765 ss.

La formazione e lo sviluppo delle nostre personalità sono incisi dalla presenza e dal rilievo dei servizi digitali che si alimentano sistematicamente di dati: la dipendenza dai dati che è una caratteristica propria delle macchine (*data dependency*[36]), si risolve ormai nella nostra dipendenza dalle macchine e quindi dallo sfruttamento dei dati in nostro favore (*data dependencies*).

Le persone dipendono dalla circolazione di dati e informazioni per l'ordinario svolgimento della propria personalità, sia come singoli, sia nelle formazioni sociali. Le implicazioni costituzionali di questa osservazione sono molteplici e rappresentano il passaggio dall'irenica – si direbbe[37] – *data-driven innovation*, alla ben più stringente dipendenza sistematica e strutturale dalla datificazione. Si tratta di una questione di diritto costituzionale[38].

Gli esempi potrebbero moltiplicarsi: ma se questa è la descrizione del contesto, si comprende perché è giuridicamente necessario rinvenire un ordine nel sistema della datificazione[39] e, progressivamente, un ordinamento costituzionale dei dati.

4. Dati e informazioni[40]

La seconda osservazione descrittiva è che esiste una grande differenza oggettiva – non sempre adeguatamente colta né dal legislatore, né dagli osservatori[41] – fra dati e informazioni.

Procediamo ancora con esempi, per introdurci al tema.

E partiamo dalla Cina[42]. Nel 2021 il legislatore cinese ha adottato due leggi molto significative: la c.d. "Data security law" (di seguito, DSL) e la c.d. "Personal information protection law" (di seguito, PIPL)[43]. Leggendo le rispettive disposizioni di legge, sembra di poter affermare che il legislatore cinese ha voluto distinguere, in modo necessariamente non casuale, tra "informazioni" (PIPL) e "dati" (DSL), e su queste due distinte nozioni ha costruito i due corpi normativi.

Si potrebbe presumere che ciò che conta, ai fini del PIPL, sia l'aspetto funzionale – l'informazione – più che il profilo strutturale – i dati –, poiché l'interesse primario del PIPL è quello di proteggere i diritti e gli interessi delle persone fisiche (artt. 1 e 3). Al contrario, quando l'interesse principale è l'interesse pubblico (la sicurezza dello Stato, che – va notato – include anche «i legittimi diritti e interessi di individui o organizzazioni», come specificato nell'art. 21 DSL), allora emerge la prospettiva della sovranità digitale dello Stato, che si basa sul riferimento alla nozione di "dati", indipendentemente dalle informazioni che incorporano. I dati intesi come entità fisica sono e devono essere sotto il controllo dello Stato (ubicazione, disponibilità, conservazione, utilizzo).

Infatti, ai fini della tutela della privacy della persona, ciò che conta non sono i "dati" intesi come entità fisica, ovvero i dati informatici, ma l'uso che se ne può fare nel contesto sociale, e quindi il significato, le informazioni che il titolare/responsabile

36. Wenfei-Geerts 2012, p. 8: «Dependencies as data quality rules. A central question concerns how we can tell whether our data have semantic errors, i.e., whether the data are dirty or clean. To this end, we need data quality rules to detect semantic errors in our data, and better still, fix those errors by using the rules. But what data quality rules should we adopt? A natural idea is to use data dependencies (integrity constraints). Dependency theory is almost as old as relational databases themselves. Since Codd [1972] introduced functional dependencies, a variety of dependency languages, defined as various classes of first-order logic sentences, have been proposed and studied. There are good reasons to believe that dependencies should play an important role in data quality management systems. Indeed, dependencies specify a fundamental part of the semantics of data, in a declarative way, such that errors emerge as violations of the dependencies».
37. Cfr. Luciani 2006.
38. Barbera 1975.
39. Cfr. Durante-Pagallo 2022.
40. Cfr., acutamente e preliminarmente, Durante 2022.
41. Si veda il contributo fondamentale di Orlando 2022, p. 14 ss.; Finocchiaro 2012.
42. Si riprende qui quanto si è potuto osservare in Calzolaio 2023, p. 197 ss., cui si rinvia per più specifici riferimenti.
43. Le norme cinesi sono reperibili in https://digichina.stanford.edu/ (traduzione non ufficiale, ma affidabile).

del trattamento può o intende estrarre dai dati nell'ambito del trattamento effettuato.

In questo senso, la "informazione personale" corrisponde alla nozione europea di "dati personali" a seconda dell'uso che ne viene fatto[44]: ma ai fini della protezione personale, la nozione di "informazioni personali" è più utile di quella di "dati personali", poiché tende a declinare l'applicazione della disciplina in materia in considerazione dei caratteri del trattamento concretamente svolto dal titolare e, contemporaneamente, del rischio effettivo per l'interessato.

La questione si fa ancora più interessante – nel diritto cinese – perché il termine "informazione" viene abbandonato e sostituito dal concetto di "dato" quando entra in gioco l'interesse pubblico per la sicurezza e la sovranità digitale dello Stato.

In questo caso, infatti, lo Stato (cinese) intende tutelarsi proprio dalla possibilità che altri soggetti, anche altri Stati, possano avvalersi di mezzi computazionali che vanno oltre quanto prevedibile o ragionevole (in termini di tempi, costi, competenze professionali, numero di persone dedicate)[45] al fine di ricavare informazioni (strategiche) dai dati (informatici): le informazioni che uno Stato o una entità straniera possono ricavare dalla analisi dei dati "cinesi" possono infatti anche essere ulteriori e diverse da quelle di cui lo Stato cinese stesso è in possesso attraverso l'ordinario sfruttamento di quei dati.

In altri termini, l'utilizzo della nozione di "dato" al fine di proteggere gli interessi nazionali cinesi rappresenta una forma di principio di precauzione dalla estrazione di informazioni dai dati "cinesi", con tecnologie presenti o future non necessariamente conosciute dall'ordinamento cinese, svolta da soggetti estranei alla Cina e con tempi, modi, esiti che possono generare una asimmetria informativa fra Cina e soggetti stranieri. Le norme cinesi si concentrano sul "dato" perché il processo di *data mining*, sviluppato in modo non controllato dalle autorità nazionali cinesi, può condurre a informazioni inedite, imprevedibili e strategiche per (e contro) l'ordinamento cinese.

In questo caso, quindi, è più che comprensibile che la disciplina dello Stato tuteli i "dati", e non le "informazioni": si tratta di una forma di tutela anticipata del rischio[46], fondata su una valutazione assiologica (cinese) di carattere giuridico-costituzionale.

In conclusione, l'ordinamento dei dati cinese ci dimostra plasticamente il primo profilo della distinzione tra dati e informazioni (che peraltro è piuttosto familiare al costituzionalista che può ricorrere all'analogia con i concetti di disposizione e norma).

Ma un esempio ancora più interessante, e a me familiare[47], è stato rappresentato in un recente contributo, facendo leva su consolidati studi ed evidenze scientifiche. In sostanza, tutto il meccanismo tecnologico della blockchain, i suoi profili di sicurezza e di progressione dei blocchi, si basa sulla (dispendiosissima, sul piano strettamente energetico) capacità computazionale delle macchine, volta a decodificare dati sempre più complessi per raggiungere informazioni significative per la

44. Cfr. OECD 2014, pp. 14-16; Abrams 2014.

45. … quelli qui citati sono i criteri in base ai quali è possibile ritenere che dei dati sono stati anonimizzati (perdendo quindi l'attributo di "personali"): si tratta per l'appunto di un criterio di tipo stipulativo e non oggettivo. Cfr. considerando n. 26, GDPR: «Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato». Comunque sul tema v. sempre D'Acquisto-Naldi 2017 e volendo anche Calzolaio 2017, p. 605, ove si lega il tema alla previgente dir. 95/46/CE, cons. 26, ed alla intepretazione dei concetti di anonimizzazione e pseudonimizzazione dell'allora Gruppo art. 29.

46. Sul tema, ora, acutamente, Longo 2024; per connessione, v. anche Longo 2024a.

47. Autorevolmente: E-Calzolaio 2023. Il saggio affronta il tema della qualificazione dei dati come beni e del rapporto sussistente fra persona e dati, ma a tal fine sviluppa inizialmente una descrizione pregevole e chiarissima dei caratteri delle blockchain, che nel testo si è sintetizzata.

catena digitale e per i suoi utenti. Il passaggio fra dato e informazione, e l'intermediazione di una chiave, determina la sicurezza strutturale dell'informazione (conosciuta dal solo titolare della chiave), mentre il dato può circolare liberamente (poiché non può essere decodificato).

Questo esempio conferma la distinzione proposta fra dato e informazione, ma aggiunge un tassello importante: affinché il dato sia tradotto in informazione è necessaria – in ambiente digitale – l'intermediazione della macchina e della sua capacità computazionale (hardware e software).

Nel passaggio fra dato e informazione, quindi, c'è un consumo di energia, che pone – come nel caso della blockchain – un tema di sostenibilità ambientale della evoluzione digitale[48], almeno per quanto concerne il modello di sicurezza della blockchain.

Inoltre, il fatto dell'inevitabile intermediazione della macchina pone il problema del titolo di appartenenza del dato e dell'informazione alla persona, alla macchina (e al suo titolare, se la macchina non ha – come per ora non ha – soggettività giuridica) e al fornitore di servizi, delle relative responsabilità e della configurazione del rapporto giuridico intercorrente fra questi "soggetti", in modo che ancora non appare risolto[49].

Infine, passiamo alla più pedestre realtà della attuazione del PNRR e quindi del PSN (Polo strategico nazionale[50]), cioè del cloud nazionale dei dati: la localizzazione dei cloud è nazionale, la tecnologia di base è americana, la criptografia delle informazioni è sviluppata a livello nazionale a seconda della tipologia di dati e servizi coinvolti (ordinari, critici, strategici)[51]. Quindi, in ipotesi, le aziende americane fornitrici della tecnologia su cui si fonda il cloud nazionale potrebbero venire in possesso dei "dati" contenuti nel cloud, ma ciò non implicherebbe la conoscenza delle "informazioni" portate dai dati, ché sono crittografate e dovrebbero essere conoscibili solo dai titolari italiani delle relative chiavi crittografiche esclusive. Si può pertanto porre una cesura nel rapporto fra dato e informazione, tale da escludere la capacità delle macchine di risalire dal dato all'informazione.

Possiamo quindi sintetizzare tre passaggi, in merito al rapporto fra dati e informazioni:

1) il dato è la base materiale ("la rappresentazione digitale"[52]) del suo significato, che chiamiamo informazione: a seconda di quanto sia rilevante (sul piano del valore giuridico-costituzionale) l'informazione che si può trarre dal dato, ovvero di quanto sia prezioso il dato e rischiosa la sua circolazione, è possibile anticipare la tutela al dato oppure si può consentire al dato di circolare e proteggere l'informazione che se ne ricava, oppure ancora non proteggere né l'uno né l'altra, perché è un bene che il dato e l'informazione circolino – quest'ultima dovrebbe essere la logica dei dati pubblici sul modello del cd. FOIA;
2) per ottenere una informazione dal dato è necessaria l'intermediazione della macchina; ciò comporta un dispendio di energia e, quindi, si lega il tema della evoluzione digitale alla sostenibilità ambientale[53], che può divenire un legittimo criterio di orientamento normativo, di rilievo costituzionale, dello sviluppo delle tecnologie;
3) nel rapporto fra dato e informazione, intermediato dalle macchine, esistono una molteplicità di strumenti tecnici volti a garantire l'improbabilità (e stipulativa impossibilità) che dal dato la macchina riesca a risalire all'informazione (crittografia) e strumenti organizzativi volti ad impedire che macchine non autorizzate possano analizzare dati protetti (obblighi di localizzazione, ad esempio). L'utilizzo di tali strumenti può essere combinato, ma soprattutto deve essere disciplinato in modo ordinato.

Nel contesto della dipendenza dai dati, la distinzione fra dati e informazioni assume un rilievo indiscutibile sia nei rapporti fra persone fisiche, sia nei rapporti di servizio e di consumo e cioè fra consumatore/utente e impresa, sia nei rapporti fra

48. Come puntualmente documenta E-Calzolaio 2023, spec. p. 92 e nota 15.

49. Ma su questo appunto si esercita la dottrina civilistica: E-Calzolaio 2023, p. 287 ss.

50. V. il sito ufficiale.

51. La disciplina e le vicende del PSN sono ben spiegate da Macrì 2022.

52. Cfr. *Data governance act*, art. 2, par. 1, n. 1), v. Iannuzzi 2024.

53. Cfr. Orofino 2023.

privati e soggetti pubblici, sia nei rapporti fra soggetti pubblici, ivi compresi i rapporti fra ordinamenti statuali.

Questa distinzione è un architrave ordinamentale di tutta la regolazione del diritto dei dati, anche se le difficoltà e incertezze definitorie non sempre riescono a farla emergere chiaramente, e in ciascun ambito sarà declinata seguendo gli equilibri e la tradizione giuridica dei diversi settori (diritto privato in senso stretto e diritto dei consumatori, diritto pubblico, diritto della concorrenza, diritto amministrativo e delle amministrazioni pubbliche, diritto delle telecomunicazioni, ecc.).

Per essere più chiari, le disposizioni in materia di trasparenza amministrativa (d.lgs. 33/2013) implicano di norma che, nell'adempimento degli obblighi di pubblicazione, dati e informazioni coincidano: il dato deve essere conoscibile a tutti e quindi non può essere pubblicato nella sezione amministrazione trasparente in una modalità o in un formato che renda non conoscibile l'informazione che il dato porta, ad esempio, richiedendo all'utente di dotarsi di un software proprietario per poter essere conosciuto.

In pressoché tutti gli altri casi è, invece, esattamente il contrario (o comunque ciascun soggetto può regolarsi, in assenza di norme specifiche, come meglio ritiene). Se invece l'informazione deve restare riservata o segreta, poiché l'ordinamento lo impone o l'interesse tutelato del soggetto che ne ha la disponibilità lo richiede, allora si utilizzeranno i metodi tipici per garantire riservatezza e segretezza: sul versante del dato, la localizzazione, la limitazione all'accesso o al trasferimento, il controllo da parte delle autorità preposte della circolazione del dato come tale; sul versante dell'informazione (i.e., del rapporto fra dato e informazione), la crittografia o strumenti di anonimizzazione o strumenti di pseudonimizzazione, o altri modelli organizzativi, a seconda dei casi.

In conclusione, possiamo distinguere un piano ordinamentale e un piano costituzionale.

Sul piano ordinamentale – cioè delle nozioni di base per qualsiasi forma di regolazione, pubblica o privata o pubblico-privata – la distinzione fra dato e informazione è basilare. In questo ambito occorre uno sforzo di osservazione e descrizione delle fattispecie concrete, da utilizzare per una corretta regolazione.

Sul piano costituzionale, nel rapporto fra dati e informazioni vale quel che affermava Norberto Bobbio nel noto saggio *La democrazia e il potere invisibile* del 1980: in democrazia, il governo si esprime attraverso un "potere visibile" e, pertanto, nello stato costituzionale, per quanto concerne i poteri pubblici, «la pubblicità è la regola, il segreto è l'eccezione». Qualche anno dopo, Paolo Barile apriva il proprio saggio *Democrazia e segreto* del 1987 affermando che «valgono regole opposte circa il segreto nel pubblico ed il segreto nel privato. L'apparato della democrazia ha per regola la trasparenza, ed il segreto costituisce una eccezione. I diritti costituzionalmente garantiti al soggetto privato in democrazia (la libertà nella comunità [n.d.a., *da tenere a mente: la libertà nella comunità*]) hanno per regola la privacy, e per eccezione la pubblicità».

5. Informazioni (dati) personali, informazioni (dati) non personali, dati importanti/critici, dati strategici

Una volta specificato il contesto ("dipendenza dai dati" e distinzione "genetica" fra dati e informazioni), possiamo addentriamoci allora nella tipologia, in senso oggettivo, dei dati e delle informazioni.

I dati sono – essenzialmente – la rappresentazione digitale di fatti e atti. Le informazioni che se ne traggono possono riguardare una persona fisica, identificata o identificabile, e allora sono dati personali, ovvero possono non riguardare una persona fisica, ed essere dati non personali.

Ma questa distinzione binaria (di cui siamo debitori innanzitutto del diritto europeo, poiché ci ha introdotto alla comprensione, alla regolazione e alla ricerca nel settore del diritto dei dati e del digitale), ben presto si è rivelata insufficiente a descrivere la tipologia in senso oggettivo dei dati, poiché l'ambiente digitale non si esaurisce nel discrimine fra dati personali e non personali.

E non è sufficiente affermare – come pure sembrerebbero voler dire il GDPR e il Regolamento sui dati non personali[54] – che un dato non personale può circolare liberamente, perché semplicemente non è così.

54. Torregiani 2020.

Nell'ordinamento dei dati cinese, ad esempio, è adottata una specifica tripartizione dei dati (nel DSL): dati, dati importanti, dati di interesse nazionale strategico[55].

La nozione di "dati importanti" appare davvero molto rilevante e cambia la prospettiva della regolazione, poiché identifica una specifica categoria della materia del diritto dei dati.

La legge cinese ci rivela che il regime dei dati non è determinato unicamente dal fatto di essere qualificati come "dati personali" (quindi protetti) o "dati non personali" (quindi soggetti a libera circolazione) secondo quanto sembrava prevedere – nella consueta prospettiva limitante del mercato unico digitale – l'ordinamento europeo.

La legge cinese afferma chiaramente che i dati e gli insiemi di dati, anche non personali, possono assumere valore strategico e possono avere diversi livelli di importanza per lo sviluppo economico e sociale e per la sicurezza dello Stato e dei diritti delle persone – a prescindere dalla loro qualificazione come dati personali o non personali. Le categorie cinesi sono tre, non due: informazioni personali, dati, dati importanti e quest'ultima è una categoria *autonoma e trasversale* rispetto alle altre (all'interno della quale si collocano anche i *core national data*, ovvero dati di interesse strategico nazionale).

A pochi mesi di distanza dalla adozione di queste leggi cinesi (rispettivamente settembre, DSL, e novembre, PIPL, del 2021), in Italia, la costituzione del Cloud nazionale[56] poneva esattamente gli stessi problemi di classificazione di dati e servizi pubblici e l'Agid, con proprio regolamento[57], richiedeva alle amministrazioni pubbliche di classificare i propri dati e servizi «sulla base della loro caratterizzazione, nelle seguenti tre classi:

a. *strategici*, se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale;
b. *critici*, se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
c. *ordinari*, qualora la loro compromissione non determini i pregiudizi di cui alle lettere a) e b)»

(così art. 3, c. 3, Regolamento Agid cd. *Servizi Cloud*).

Solo per completezza si ricorda – rinviando ancora al testo prezioso di Indra Macrì[58], che spiega con chiarezza procedure che altrimenti sarebbe estremamente faticoso ricostruire, da parte di un giurista, sulla base dei soli atti, normativi e non, delle diverse autorità implicate – che a partire da questa *classificazione di dati e servizi* si realizza, in parallelo, una *qualificazione dei servizi cloud* (cloud pubblico qualificato e non qualificato, cloud pubblico criptato, cloud privato/ibrido su licenza e privato qualificato), in forza della quale al livello di "sensibilità" dei dati corrisponde la possibilità di valersi di cloud recanti maggiori garanzie in termini di localizzazione, vigilanza esterna, crittografia dei dati[59]. Il Polo strategico nazionale (PSN) che è in fase di realizzazione viene utilizzato proprio per consentire la migrazione dei dati delle pubbliche amministrazioni in cloud qualificati e sicuri e, per i dati strategici, localizzati in Italia[60].

Vi sono alcuni profili da rimarcare in merito alla classificazione in senso oggettivo dei dati.

Il primo aspetto è che alcuni principi e indirizzi normativi – come quello dell'altruismo dei dati (su cui, in questa sezione monografica, v. il contributo di Elia Cremona[61]), o del più generale favore per la condivisione dei dati per finalità di sviluppo,

55. Sia consentito rinviare a Calzolaio 2023, p. 209 ss.

56. Su cui v. ancora Macrì 2022, p. 293 ss.

57. AGID, determinazione n. 628, 15 dicembre 2021, recante Adozione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione".

58. Macrì 2022, pp. 319-325.

59. Cfr. art. 33-*septies*, d.l. 179/2012.

60. Ci eravamo per l'appunto posti il problema della localizzazione dei dati, qualche tempo fa, in questa Rivista: cfr. Calzolaio 2021.

61. Cremona 2023.

ricerca ecc.[62] – si possono applicare, di norma, *in via residuale* alle categorie di dati non personali, non critici, non strategici. Che senso avrebbe, altrimenti, far classificare i dati alle amministrazioni pubbliche come critici e/o strategici e di conseguenza adottare modelli di cloud qualificati per mantenere i dati (e i servizi) sicuri, per poi consentirne la condivisione o la diffusione sistematica?

D'altra parte, proprio il regime di sicurezza che consegue alla classificazione dei dati delle amministrazioni come critici o strategici impone che i criteri regolamentari siano applicati in modo uniforme sull'intero territorio nazionale[63], per evitare che le amministrazioni classifichino in modo diverso dati e servizi analoghi (o viceversa), ingenerando una evitabile confusione e rischi per la sicurezza.

La quadripartizione classificatoria qui proposta si pone al punto di confluenza fra l'ordinamento (europeo) dei dati personali e l'ordinamento costituzionale dei dati e, in questo ambito, il diritto (europeo) alla protezione dei dati personali si incontra con le esigenze nazionali attinenti alla cd. sovranità digitale[64] (su cui si veda, in questa sezione monografica, il contributo di Stefano Torregiani[65]), sotto il profilo della organizzazione delle pubbliche amministrazioni e della tutela dei diritti dei cittadini italiani.

6. Dati, dati sintetici e sistema dell'informazione ibrido: l'essenziale è invisibile agli occhi?

«… my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits»[66].

Questa è una delle preoccupazioni principali che esprime il presidente Biden nel suo ordine esecutivo Executive Order (E.O.) *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* del 30 ottobre del 2023.

Questo aspetto interessa specificamente l'ordinamento dei dati e, più specificamente, lo arricchisce ormai strutturalmente di una categoria ulteriore, che è in grado di rivoluzionare il nostro ambiente umano: i dati sintetici.

Ma procediamo per gradi.

Che cos'è l'intelligenza artificiale generativa? Secondo l'E.O. «The term "generative AI" means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content».

E cosa sono questi contenuti sintetici? Ancora secondo l'E.O. «The term "synthetic content" means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI».

Ciò significa che l'IA generativa produce per definizione contenuti sintetici – i.e., dati sintetici, informazioni sintetiche – di qualsiasi tipo (immagini, video, testi e altri contenuti digitali).

E perché mai questi contenuti sintetici dovrebbero preoccuparci, così come preoccupano il presidente Biden che vi dedica l'intero titolo 4.5 (*Reducing the Risks Posed by Synthetic Content*) del suo E.O.?

Perché sono contenuti prodotti e messi in circolazione nello spazio digitale senza che, attualmente, gli esseri umani possano distinguerli dai contenuti non sintetici – cioè dai contenuti aventi una origine effettivamente umana.

E perché questo aspetto è così rilevante? Facciamo un esempio.

Immaginiamo che un gruppo di informatici addestri un sistema di intelligenza artificiale per produrre immagini di ambienti interni ed esterni di chiese, palazzi storici, beni culturali in genere. Il sistema viene alimentato da immagini reali, le

62. Cfr. Iannuzzi 2024.

63. Si tratta di applicare i principi del coordinamento digitale unitario e di standardizzazione, indicati in Calzolaio 2016, spec. p. 196.

64. Finocchiaro 2022, pp. 809 ss.; Simoncini 2017.

65. Torregiani 2023.

66. U.S. Executive Order 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

immagazzina, le elabora, e poi comincia a produrne autonomamente a milioni – si pensi a quanta elegante creatività a basso costo per architetti, designer, mobilifici ecc.!

Queste immagini verosimili riproducono anche ambienti e beni reali: piazza San Pietro, la basilica di San Francesco di Assisi, la Tour Eiffel e così via. Queste immagini cominciano ad abitare, o ad invadere, lo spazio digitale e poi il Web.

Un giovane studente svolge una ricerca scolastica su uno di questi monumenti, quindi osserva e scarica queste immagini: sono verosimili, ma non riproducono esattamente quel monumento. Ci sono delle differenze, più o meno percettibili. Lo studente descrive l'immagine, che crede reale, e invece è verosimile, quindi contiene delle differenze con la foto reale del monumento. Lo studente, tuttavia, è certo di conoscere quel monumento sulla base delle immagini reperite e quando il professore gli fa osservare che, invece, quel monumento non ha questa o quella caratteristica che lo studente ha descritto, lo studente reagisce come se il professore negasse una realtà evidente, oggettiva. Ne nasce una discussione: entrambi sanno di avere ragione[67].

Immaginiamo ora che sia trascorso del tempo: 100 anni. E che in questi 100 anni si siano accumulate una miriade di immagini che riproducono in tutti i modi quel certo monumento in diversi momenti di tempo e altrettante ricerche: potremmo ricostruire la storia del monumento, se potessimo essere (ragionevolmente) certi che sono vere le immagini e le ricerche che ritraggono e raccontano effettivamente quel monumento così com'era tempo per tempo. Ma non possiamo più esserlo: la maggior parte delle immagini e delle ricerche sono contenuti sintetici, o ibridi, e non ritraggono e non raccontano i luoghi, ma sono prodotto – verosimile, indistinguibile immediatamente – di intelligenza artificiale generativa[68]. Non solo: i racconti delle persone viventi sullo stato dei luoghi e sulle vicende del monumento non coincidono con le immagini e le ricerche, talvolta sono contraddittori. Ne nasce una grande incertezza: nessuno si può fidare della narrazione storica.

Il primo aspetto rilevante dell'avvento pervasivo della categoria dei dati sintetici è che essi sono in grado di modificare, impercettibilmente, *l'asse terrestre della cognizione umana*[69]. Con conseguenze imprevedibili, ma certamente rischiose, nel breve, medio e lungo termine.

Per questo, l'E.O. adotta politiche immediate di *watermarking*[70] e di etichettatura di questi dati sintetici e delle relative informazioni immesse nel circuito digitale[71].

Tuttavia – e questo è il secondo aspetto – non possiamo illuderci: il sistema dell'informazione in cui siamo immersi e da cui traiamo la cognizione della realtà che ci circonda è già da tempo ibrido, cioè abitato e popolato da persone verosimili e comunicative, ma che non sono persone pur presentandosi come tali, in modo occulto (bot)[72], o in modo palese (co-pilot). L'IA generativa rappresenta un salto di qualità, in questo senso: ma

67. C'è anche un analogo esempio divertente nella filmografia di 007, *Il domani non muore mai*, 1997, in cui un miliardario del settore delle telecomunicazioni sviluppa un sistema in grado di modificare il segnale GPS, e quindi la cognizione della posizione in mare, ricevuto da una nave da guerra inglese e la fa sconfinare – ignara – nelle acque territoriali cinesi, con tutte le conseguenze del caso.

68. Cfr. Wagner-de Clippele 2023.

69. … in qualche modo l'E.O. del presidente Biden rappresenta una prima forma di disciplina della IA generativa, che appare seguire l'orientamento del giudice Thomas richiamato puntualmente da Niro 2021.

70. … secondo l'E.O.: «The term "watermarking" means the act of embedding information, which is typically difficult to remove, into outputs created by AI—including into outputs such as photos, videos, audio clips, or text—for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance».

71. L'E.O., titolo 4.5. *Reducing the Risks Posed by Synthetic Content*, fissa tappe precise per garantire l'identificazione, la rilevazione, la provenienza e l'etichettatura dei contenuti sintetici, e lo sviluppo di tecniche e standard per l'autenticazione dei contenuti. Si rinvia al testo dell'E.O. per maggior dettaglio, delle incisive misure presidenziali in merito.

72. Cfr. Tedeschi Toschi-Berni Ferretti 2023.

dobbiamo riconoscere che abitiamo in una realtà cognitivamente ibrida, fatta di relazioni con soggetti e oggetti digitali che influiscono sulla nostra percezione della realtà (si vedano i contributi in questa sezione monografica di Angela Cossiri e Arturo Di Corinto[73]), in modo ancor più incisivo se riteniamo che non sia così e di non accorgercene.

È a questo livello che si pone il problema, peraltro acutamente affrontato in dottrina, della c.d. "riserva di umanità"[74]. La realtà ibrida non consente "riserve", perché incide ineluttabilmente proprio su ciò che intendiamo per "umanità", cioè sulla nostra sfera cognitiva, sulla formazione del pensiero e della personalità[75]: lo studente del nostro precedente esempio potrebbe essere un giudice, un chirurgo, un generale, un autista, un dirigente d'azienda, una persona comunque convinta di basare le proprie azioni su una visione *oggettiva* – ma in realtà solo *oggettivizzata* – della realtà, e di essere nel giusto, di rappresentare il vero. Quindi, più che difendersi, bisogna apprendere rapidamente ad affrontare la realtà ibrida con tutti i suoi rischi epocali – come intuito rapidamente dall'E.O.

Il primo passo in tal senso è aggiornare la classificazione dei dati e delle informazioni con il riferimento esplicito agli inevitabili contenuti sintetici, ed alla pressante esigenza di determinare le modalità per renderli il più possibile sistematicamente visibili e riconoscibili agli esseri umani (e, soprattutto, ai minori).

7. Una (apparente) sosta: dati epidemiologici del Surgeon General

Nel 2023 il Surgeon General (S.G.) statunitense ha pubblicato solo due Avvisi[76].

Raccontano due distinte, ma connesse, emergenze epidemiologiche che investono la società statunitense e che – per dovere istituzionale – spetta proprio al S.G. identificare e denunciare, per tutelare e proteggere la salute pubblica degli americani.

A ormai oltre 25 anni dall'avvento della rete Internet e a oltre 15 dall'avvento dei social media, come fenomeni di massa, la società americana è investita da due fenomeni che minacciano – dati alla mano – la speranza di vita e la salute degli americani: la solitudine e l'isolamento sociale delle persone; la salute mentale dei giovani. Come si potrà verificare, si tratta di due studi seriamente documentati.

Per quanto qui interessa, in entrambi – molto più esplicitamente in quello concernente i minori, che davvero non lascia nulla di implicito (negli Stati Uniti è in atto «una crisi nazionale di salute mentale giovanile»: p. 13, righe 9-10) – si identifica un ruolo specifico dell'avvento della società digitale nel mutamento esistenziale e nel peggioramento delle condizioni socio-sanitarie che colpisce gli americani e i giovani americani.

Le azioni che sono suggerite per contrastare queste problematiche coinvolgono esplicitamente i famosi "poteri privati" della tecnologia. Ma a mio avviso vi è un profilo ancor più rilevante in questi Avvisi: essi cercano di enucleare modalità operative di azione dei poteri pubblici (e privati) americani per contrastare la solitudine e l'isolamento sociale, da un lato, e le minacce alla salute mentale dei giovani, dall'altro: queste sembrano essere le vulnerabilità della società americana più pressanti.

Sul primo versante, il S.G. suggerisce l'adozione di politiche pubbliche che favoriscano le relazioni sociali e, in particolare, il *"Connection-in-All-Policies" approach*.

È peculiare che nella patria dell'individualismo si proponga esplicitamente e come misura in grado di contrastare la diminuzione della speranza di vita delle persone sole o isolate, l'adozione sistematica di politiche pubbliche attive, in tutti i settori, volte a favorire la partecipazione delle persone ai rispettivi ambienti comunitari.

Questo aspetto colpisce, in quanto si tratta un profilo che la Costituzione italiana – forse più di quella americana – conosce e valorizza, a partire proprio dalla formula dell'art. 2 Cost.: «la "persona", per non scadere ad "individuo", va considerata non solo nella sua "immanenza" [n.d.a., *ove oggi sarebbe vittima di una realtà ibrida, che lo relega alla solitudine ed allo sbandamento cognitivo*] ma anche nella sua "apertura sociale", non solo "nell'isolamento dell'uomo dall'uomo", ma anche "nel

73. Cossiri 2023; Di Corinto 2023.

74. Cfr. Gallone 2023; Cerri 2023.

75. Richards 2015.

76. Cfr. U.S. Surgeon General 2023; U.S. Surgeon General 2023A.

legame dell'uomo con l'uomo"»[77] e i doveri di solidarietà «sono da vedere non in funzione restrittiva della libertà della persona (non come eccezioni rispetto a regole) ma in una prospettiva tale da consentirne il pieno ed armonico sviluppo»[78]; e ancora: «le formazioni sociali vengono riconosciute e garantite a livello costituzionale non come tali ma nella misura in cui consentano e favoriscano il libero sviluppo della persona (…) o nella misura in cui garantiscano la tutela di "interessi diffusi" rilevanti costituzionalmente»[79].

Sorprende quindi che, senza negare l'esigenza di modificare i modelli fatti propri dai poteri privati delle *big tech*, il S.G. muova dalla esigenza di riscoprire la dimensione ed il valore sociale dei rapporti personali (fra) privati, come rimedio a malattie e morte precoce, fra l'altro.

Sul versante della tutela della salute mentale dei minori dai social media – e come si comprende, non deve essere stato particolarmente popolare l'intitolazione stessa dell'Avviso presso le *big tech* – il S.G. rileva che, in assenza di protezioni adeguate, i bambini statunitensi sono divenuti partecipanti inconsapevoli di un esperimento decennale. Pertanto è molto più netto, stanti anche le gravi conseguenze di questa esposizione, e si richiama all'esigenza di applicare il *Safety-first approach*: «According to this principle, a basic threshold for safety must be met, and until safety is demonstrated with rigorous evidence and independent evaluation, protections are put in place to minimize the risk of harm from products, services, or goods»[80].

Vorrei osservare che fra i molteplici interventi normativi dell'Unione europea in materia di diritto dei dati e di società digitale – come emerge dalla tabella curata da Camilla Lobascio[81] – non v'è specifica attenzione a nessuno di questi due aspetti, di cui onestamente il più originale è senz'altro il primo: il recupero e la promozione delle relazioni sociali come strumento di lotta all'isolamento ed alla solitudine largamente indotti, o almeno accelerati, dall'avvento della società digitale e della datificazione.

8. Spunti conclusivi per un ordinamento costituzionale dei dati

In conclusione, si desidera sommessamente individuare, a mo' di elenco, una serie di temi di stretta, e anche classica, attinenza costituzionale che rappresentano altrettanti capitoli da scrivere per fondare un effettivo ordinamento costituzionale dei dati, che limiti e orienti il processo di datificazione: la tutela della libertà di pensiero e del libero sviluppo della personalità; l'esigenza positiva di concepire un nuovo modello di pluralismo informativo; il rischio di una regolazione eccessiva e di un accentramento di competenze tecniche in organi sostanzialmente di governo.

Il primo fra questi è stato sviluppato negli Stati Uniti da Neil Richards, con il suo volume del 2015, sulla *Intellectual privacy*: sin da allora – e sul piano tecnologico è già cambiata un'epoca – egli osservava che la protezione dei dati personali non era più solo una questione di autodeterminazione informativa, ma ormai appariva come un presidio della libera formazione del pensiero e, con esso, della personalità. La datificazione e l'asseto ibrido del sistema dell'informazione e, ormai si può affermare, della realtà, mettono davvero a rischio le funzioni cognitive dell'essere umano. La rete di relazioni sociali e la sua sistematica promozione sono un buon antidoto: ma cos'altro può proteggere la sfera di libertà della persona di fronte alle macchine intelligenti che la circondano?

Un secondo aspetto – connesso – concerne la riscoperta del significato attuale del principio del pluralismo informativo[82]. Il principio in parola[83] nasce per garantire che il sistema dell'informazione più pervasivo del tempo, quello radio-televisivo,

77. Cosi Barbera 1975, p. 106, citando Karl Marx, nella nota 14.

78. *Ibidem*, p. 106.

79. *Ibidem*, p. 109.

80. Ivi compresa l'azione di «Pursue policies that further limit access – in ways that minimize the risk of harm – to social media for all children, including strengthening and enforcing age minimums».

81. Lobascio 2023.

82. Cfr. Caterina 2023, p. 19 ss.

83. Albanesi-Valastro-Zaccaria 2023, pp. 35-37.

vedesse protagonisti una pluralità di soggetti, nessuno dei quali in posizione dominante (pluralismo esterno) in modo che vi fossero più voci diverse ad operare nel sistema dell'informazione. D'altra parte, seppure rivolto principalmente alla radio-tv pubblica, si è anche affermato il principio del pluralismo interno, inteso nel senso di offrire, all'interno della medesima emittente, il più largo spazio a opinioni, tendenze e culture diverse e rappresentative del pluralismo sociale. Nell'era dell'iperconnessione ibrida e delle piattaforme digitali, cosa si intende per pluralismo informativo? Come si possono coniugare (o limitare reciprocamente) datificazione, iperconnessione e esigenze personali, sociali e democratiche di pluralismo informativo (o, se si preferisce, di libertà passiva di informazione)? Il nemico di un tempo (la tradizionale scarsità di risorse informative, frequenze ed editori) appare superato, ed anzi oggi appare l'eccesso e la velocità di informazione un ostacolo al pluralismo informativo: forse un aiuto potrebbe arrivare proprio da una limitazione della velocità delle informazioni e da un design orientato al pluralismo informativo di strumenti di intelligenza artificiale che ci supportino? Si possono applicare modelli di valutazione del rischio anche a questo ambito, per suggerire un quadro plurale qualitativamente e sostenibile quantitativamente di informazioni?

Il terzo aspetto – come emerge dalla citata Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme – concerne i rischi di coordinamento e integrazione della cospicua regolazione europea sopravvenuta nell'ultimo biennio, sia rispetto all'esperienza – positiva! – maturata nella applicazione del GDPR, sia rispetto alla effettiva capacità regolatoria dei nuovi fronti aperti, dal DGA/DA, al delicato e rimaneggiato IA Act. Un focus particolare concerne poi l'esigenza di una efficace allocazione delle funzioni, anche di carattere tecnico, strettamente connesse, se non proprio assimilabili in questo campo, con quelle regolatorie[84]. Come osserva bene Federico Serini[85], la regolazione della società digitale si sviluppa innanzitutto attraverso la fissazione degli standard internazionali che governano i diversi aspetti alla base della produzione delle tecnologie, che spesso sfuggono anche al livello europeo.

In ogni caso, come si avvertiva già qualche tempo fa, siamo ormai lontani dalla regolazione della società digitale come ordine spontaneo[86].

This work has been funded by the European Union - NextGenerationEU under the Italian Ministry of University and Research (MUR) National Innovation Ecosystem grant ECS00000041 - VITALITY - CUP E13C22001060006

Riferimenti bibliografici

L. Abba, A. Lazzaroni, M. Pietrangelo (2022) (a cura di), *La internet governance e le sfide della trasformazione digitale*, Editoriale scientifica, 2022

M. Abrams (2014), *The Origins of Personal Data and its Implications for Governance*, The Information Accountability Foundation, March 2014

E. Albanesi, A. Valastro, R. Zaccaria (2023), *Diritto dell'informazione e della comunicazione*, Cedam, 2023

M.R. Allegri (2018), *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2018

V. Amenta (2015), *Internet governance eco-system: un'utopia globale? Dal modello multi-stakeholders al modello multi-equal-stakeholders*, Giuffrè, 2015

84. Sia consentito rinviare, a questo riguardo, a Calzolaio 2024.

85. Serini 2023.

86. Cfr. Bifulco 2018, spec. p. 394 ss.

C. Anderson (2008), *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, in "Wired", 23 June 2008

M. Arnese, F. Walsingham (2020), *Perché Ericsson, Nokia, Cisco e Microsoft brinderanno in Italia col 5G,* in "Start Magazine", 16 luglio 2020

T.G. Ash (2023), *Patrie*, Garzanti, 2023

A. Barbera (2020), *Prefazione*, in U. Ruffolo (a cura di), "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffré, 2020

A. Barbera (2015), *Costituzione della Repubblica italiana*, in "Enciclopedia del Diritto", Giuffrè, 2015

A. Barbera (2010), *Ordinamento costituzionale e carte costituzionali*, in "Quaderni costituzionali", 2010, n. 2

A. Barbera (1975), *Articolo 2 Cost.*, in G. Branca (a cura di), "Commentario della Costituzione. Artt. 1-12. Principi fondamentali", Zanichelli, 1975

E. Bassi (2022), *Dati, sovranità, nuovi modelli di governance*, in M. Durante, U. Pagallo (a cura di), "La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società", Mimesis, 2022

M. Bassini (2019), *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Aracne 2019

F. Bechis, R. Mieli (2019), *La nuova via della seta e il 5G. Gli obiettivi della Cina e i rischi per l'Italia*, Dossier del Machiavelli, n. 14, 21 marzo 2019

C. Bergonzini (2023), *"Prova a prendermi". Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale?*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

R. Bifulco (2018), *Intelligenza artificiale, internet e ordine spontaneo*, in F. Pizzetti, "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

V. Boncinelli (2021), *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in "Rivista italiana di informatica e diritto", 2021, n. 1

E. Bruti Liberati (2023), *Poteri privati e nuova regolazione pubblica*, in "Diritto pubblico", 2023, n. 1

E. Calzolaio (2023), *Beni digitali e proprietà fra civil law e common law*, in "Rivista critica di diritto privato", 2023, n. 3

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in corso di pubblicazione, Giappichelli, 2024

S. Calzolaio (2023), *Dalla protezione dei dati personali all'ordinamento dei dati (l'evoluzione del diritto cinese e del diritto europeo dei dati)*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

S. Calzolaio (2021), *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Calzolaio (2021a) (a cura di), *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Calzolaio (2018), *Recensione a: "Neil Richards, Intellectual privacy. Rethinking civil liberties in the digital age, Oxford University Press, 2017"*, in "Giornale di storia costituzionale", 2018, n. 36

S. Calzolaio (2017), voce *Protezione dei dati personali*, in "Digesto delle Discipline pubblicistiche", Aggiornamento, Utet Giuridica, 2017

S. Calzolaio (2016), *Digital (and privacy) by default. L'identità costituzionale dell'amministrazione digitale*, in "Giornale di storia costituzionale", 2016, n. 1

B. Caravita (2020), *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo (a cura di), "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffrè, 2020

C. Caruso (2023), *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in "Quaderni costituzionali", 2023, n. 3

M. Castells (2009), *Comunicazione e potere*, UBE, 2009

E. Caterina (2023), *La comunicazione elettorale sui social media tra autoregolazione e profili di diritto costituzionale*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

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

A.S.Y. Cheung, Y. Chen (2022), *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, in "Law & Social Inquiry", 2022, n. 11

Y.M. Citino (2023), *Social scoring e città distopica: la profilazione del cittadino con finalità di policy urbana alla prova dei valori costituzionali*, in G. Allegri, L. Frosina, A. Guerra, A. Longo (a cura di), "La città come istituzione, entro e oltre lo Stato", Sapienza editrice, 2023

J. Cohen (2019), *Between Truth and Power. The Legal Construction of Informational Capitalism*, Oxford University Press, 2019

G.L. Conti (2022), *Contratto sociale e Grundnorm al tempo degli unicorni*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022

F. Cossiga, P. Chessa (2007), *Italiani sono sempre gli altri, Controstoria d'Italia da Cavour a Berlusconi*, Mondadori, 2007

A. Cossiri (2023), *Le campagne di disinformazione nell'arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Costantino (2023), *La c.d. cittadinanza digitale,* in "Diritto pubblico", 2023, n. 1

E. Cremona (2023), *Quando i dati diventano beni comuni: modelli di* data sharing *e prospettive di riuso*, in "Rivista italiana di informatica e diritto", 2023, n. 2

M. Cuomo (2023), *La tutela del diritto alla disconnessione. Fonti, limiti e prospettive*, in "Lavoro Diritti Europa", 2023, n. 3

G. D'Acquisto (2021), *Intelligenza artificiale. Elementi*, Giappichelli, 2021

G. D'Acquisto, M. Naldi (2017), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017

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

G. De Gregorio, N. Stremlau (2020), *Internet Shutdowns and the Limits of Law*, in "International Journal of Communication", vol. 14, 2020

A. de Tocqueville (2005), *La democrazia in America*, (a cura di) G. Candeloro, RCS libri, 2005

A. Di Corinto (2023), *Netwar, come cambia l'hacktivismo nella guerra cibernetica*, in "Rivista italiana di informatica e diritto", 2023, n. 2

G. Di Cosimo (2023) (a cura di), *Processi democratici e tecnologie digitali*, Giappichelli, 2023

V. Dubal (2023), *On algorithmic wage discrimination*, in "Columbia Law Review", vol. 123, 2023, n. 7

M. Durante (2022), *Il Potere computazionale: dalle informazioni ai dati*, in M. Durante, U. Pagallo (a cura di), "La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società", Mimesis, 2022

M. Durante, U. Pagallo (2022) (a cura di), *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Mimesis, 2022

R. Eldan, M. Russinovich (2023), *Who's Harry Potter? Approximate Unlearning in LLMs*, in arXiv, 2023

P. Elmer-Dewitt (1993), *First Nation in Cyberspace*, in "Time", 6 December 1993

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

G. Finocchiaro (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012

L. Floridi (2018), *The Semantic Capital: Its Nature, Value, and Curation*, in "Philosophy & Technology", vol. 31, 2018, n. 4

J.O. Freuler (2023), *Datafication, identity, and the reorganization of the category individual*, in "Temple Law Review", vol. 95, 2023, n. 4

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

K. Geddes (2023), *The Death of the Legal Subject*, in "Vanderbilt Journal of Entertainment & Technology Law", vol. 25, 2023, n. 1

Y. Guerra (2023), *Il fenomeno delle smart city come esempio di co-regolazione delle nuove tecnologie. La democrazia locale di fronte alle sfide globali*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

S. Gunasekar et al. (2023), *Textbooks Are All You Need*, in arXiv, 2023

W. Hartzog, N. Richards (2022), *The surprising virtues of data loyalty*, in "Emory Law Journal", vol. 71, 2022, n. 5

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act*, in corso di pubblicazione, Giappichelli, 2024

A. Iannuzzi (2024a), *Le fonti del diritto per la disciplina della società digitale come affermazione della sovranità digitale europea*, in corso di pubblicazione, Giappichelli, 2024

P. Khanna (2016), *Connectography. Le mappe del futuro mondiale*, ed. it. Fazi, 2016

M.A. Lemley (2021), *The splinternet*, in "Duke Law Journal", vol. 70, 2021

C. Lobascio (2023), *Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme,* in "Rivista italiana di informatica e diritto", 2023, n. 2

O. Lobel (2021), *Biopolitical opportunities between datafication and governance*, in "Notre Dame Law Review Reflection", vol. 96, 2021

E. Longo (2024), *La disciplina del rischio digitale*, in corso di pubblicazione, Giappichelli, 2024

E. Longo (2024a), *La sicurezza nel ciberspazio. La disciplina della cybersecurity nell'Unione europea e in Italia*, in corso di pubblicazione, Giappichelli, 2024

M. Luciani (2006), *Costituzionalismo irenico e costituzionalismo polemico*, in "Giurisprudenza costituzionale", 2006, n. 4

I. Macrì (2022), *Digitalizzazione, innovazione e sicurezza nella P.A.*, Wolters Kluwer, 2022

M. Manetti (2023), *Internet e i nuovi pericoli per la libertà di informazione*, in "Quaderni costituzionali", 2023, n. 3

M. Manetti (2020), *Regolare Internet*, in "Media Laws", 2020, n. 2

J. Marinotti (2022), *Data Types, Data Doubts & Data Trusts*, in "New York University Law Review Online", vol. 97, 2022

M. Micheli, M. Ponti, M. Craglia, A. Berti Suman (2020), *Emerging models of data governance in the age of datafication*, in "Big data & society", 2020, n. 2

G. Mobilio (2021), *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021

A. Morrone (2023), *Sul «ritorno dello Stato» nell'economia e nella società*, in "Quaderni costituzionali", 2023, n. 2

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3

OECD (2014), *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21 March 2014

S. Orlando (2022), *Data vs capta: intorno alla definizione di dati*, in "Nuovo diritto civile", 2022, n. 4

M. Orofino (2023), *Le due transizioni, digitale e verde, nel c.d. pacchetto digitale europeo*, in "Astrid Rassegna", 2023, n. 10

J. Perry Barlow (1996), *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, 8 February 1996

M. Pierri (2019), *Con il 5G cinese a rischio la condivisione di informazioni con gli Usa. L'avvertimento di Eisenberg*, 1 aprile 2019

F. Pizzetti (2018), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in Id., "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

G.M. Riccio (2002), *La responsabilità civile degli internet providers*, Giappichelli, 2002

N. Richards (2015), *Intellectual Privacy. Rethinking civil liberties in the digital age*, Oxford University Press, 2015

G.M. Salerno (2018), *Le garanzie della democrazia*, in "Rivista AIC", 2018, n. 3

G. Scorza (2022), *In principio era internet e lo immaginavamo diverso*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022

F. Serini (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Serini (2022), *La protezione dei dati personali tra Giappone e Unione europea*, Aracne, 2022

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2

A. Simoncini (2020), *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta (a cura di), "Il Diritto dell'ammnistrazione pubblica digitale", 2020

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

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

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

C.P. Sundquist (2023), *Surveillance Normalization*, in "Harvard Civil Rights-Civil Liberties Law Review", vol. 58, 2023

A. Tedeschi Toschi, G. Berni Ferretti (2023), *Il contrasto legislativo ai socialbot. Alcuni spunti per una riforma in Italia*, in "Rivista italiana di informatica e diritto", 2023, n. 1

L. Torchia (2023), *Lo Stato digitale*, il Mulino, 2023

S. Torregiani (2023), *Il* Data Act*: una versione europea del* Data Nationalism*?*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18

U.S. Surgeon General (2023), *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023

U.S. Surgeon General (2023a), *Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory*, 2023

G.E. Vigevani (2023), *Piattaforme digitali private, potere pubblico e libertà di espressione*, in "Diritto costituzionale", 2023, n. 1

A. Wagner, M.-S. de Clippele (2023), *Safeguarding Cultural Heritage in the Digital Era – A Critical Challenge*, in "International Journal of Semiotic Law", 2023, n. 36

F. Wenfei, F. Geerts (2012), *Foundations of data quality management*, Springer Nature, 2012

L. Zorloni (2024), *I blackout di internet minacciano le elezioni 2024,* in "Wired", 10 febbraio 2024

S. Zuboff (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0132 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Camilla Lobascio

Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme

Il governo dei dati è stato in cima all'agenda normativa dell'Unione europea per più di un decennio ed ha avuto origine con la riforma delle norme sulla protezione dei dati, nel 2012, la quale ha portato poi allo sviluppo di numerosi strumenti regolatori che sono stati proposti ed adottati, negli ultimi quattro anni, all'interno della strategia europea dei dati. L'obbiettivo della strategia, tenendo conto del valore economico che i dati detengono, è quello di portare l'Unione ad essere leader in una società data-driven, a beneficio di imprese, cittadini e amministrazioni pubbliche.
La presente tabella, senza pretesa di esaustività, ha lo scopo di agevolare lo studio e il reperimento di materiali normativi, perciò indica le principali disposizioni del diritto europeo dei dati e delle piattaforme digitali, vigente o ancora in fase di discussione, con specifico link al sito ufficiale dell'Unione europea, ove è possibile approfondire i lavori preparatori e reperire altro materiale ufficiale.

Diritto europeo – Diritto dei dati – Data governance – Intelligenza artificiale

Summary table of the evolution of European data and platform law

Data governance has been on top of the European Union regulatory agenda for over a decade, starting with the 2012 data protection reform and culminating in the avalanche of other regulatory instruments that have been proposed and adopted in the past four years within the European Data Strategy. The strategy's plan is to make the EU a leader in a data-driven society for the benefit of businesses, citizens, and administrations, considering the nature of data as an economic good.
The presented table, without any claims of exhaustiveness, aims at facilitating the study and retrieval of normative production and thus lists the main provisions of European data and digital platform law, either in force or still under discussion, with specific links to the official website of the European Union, where it is possible to delve into the preparatory work and find other official materials.

European Law – Data Law – Data Governance – Artificial Intelligence

L'Autrice è dottoranda in "Diritto e innovazione" presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

La materia relativa alla data governance (o governo dei dati) è stata in cima all'agenda normativa dell'Unione europea per più di un decennio a partire dal 25 gennaio 2012, anno in cui la Commissione ha adottato un pacchetto di misure per la riforma delle norme dell'Unione in materia di protezione dei dati, che comprendeva sia una proposta di regolamento contenente il quadro normativo generale in materia di protezione dei dati, sia una proposta di direttiva sulla protezione dei dati nel settore delle attività di contrasto[1].

La Commissione, a partire dal 2016, ha già intrapreso diverse iniziative, tra cui si ricorda l'istituzione da parte dell'Unione europea di uno dei più solidi quadri per garantire ai suoi cittadini la fiducia digitale, il regolamento generale sulla protezione dei dati personali (GDPR)[2]. Sono da segnalare altre iniziative che hanno dato una spinta allo sviluppo dell'economia dei dati, ovvero il regolamento sulla libera circolazione dei dati non personali[3], il regolamento sulla cibersicurezza[4], e la direttiva relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico[5].

Il modello europeo di protezione dei dati ha perseguito, negli anni, una molteplicità di obbiettivi. La volontà è stata quella di diventare un riferimento per una società che, grazie ai dati, dispone degli strumenti necessari per adottare decisioni migliori, sia a livello imprenditoriale che pubblico. Per rendere concreta tale ambizione, l'Ue può ora fare affidamento sia su un quadro giuridico solido, in termini di protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, sia sul suo mercato interno, caratterizzato da imprese competitive (di ogni dimensione) e da una base industriale piuttosto diversificata[6].

Nell'ampio contesto normativo europeo si è aggiunta, più recentemente, anche la strategia europea per i dati, presentata dalla Commissione europea il 19 febbraio 2020, il cui scopo è quello di delineare obbiettivi e linee di intervento per realizzare misure politiche e investimenti a sostegno dell'economia dei dati fino al 2025[7].

Il grande impatto delle discipline europee, in grado di sviluppare una influenza normativa a livello globale, dovuto al peso del mercato europeo e in coerenza con gli interessi dell'Unione europea, va a costituire il fenomeno denominato come "Brussels effect"[8]. Attualmente è un numero piuttosto esiguo di imprese tecnologiche non-europee (*big tech*) a detenere il pieno controllo sulla maggior parte dei dati disponibili ma, con il recente regolamento europeo sui dati entrato in vigore a gennaio 2024, la Commissione mira a rendere disponibile per l'uso un maggior numero di dati e a stabilire norme su chi può utilizzarli e accedervi e per quali scopi in tutti i settori economici dell'Ue.

1. Cfr. la *Sintesi del parere del Garante europeo della protezione dei dati del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati* pubblicata in GUCE 2012/C 192/05 (il testo completo del parere è reperibile in inglese, francese e tedesco nel sito web del GEPD).
2. Regolamento (UE) 2016/679.
3. Regolamento (UE) 2018/1807.
4. Regolamento (UE) 2019/881.
5. Direttiva (UE) 2019/1024.
6. Commissione europea, "Una strategia europea per i dati", doc. COM(2020) 66 del 19 febbraio 2020.
7. Iannuzzi 2021.
8. Calzolaio 2017, p. 612.

Nel contesto descritto è chiaro come i dati si siano affermati come "bene economico", capaci di creare ricchezza per la società, prestare capacità di controllo ai cittadini e diffondere fiducia alle imprese.

La seguente tabella si propone l'obbiettivo di fornire un elenco, di semplice consultazione, disposto in ordine cronologico, delle principali normative europee in materia di governo dei dati che sono state sviluppate negli ultimi dieci anni.

	forma	procedura	termini rilevanti
	Regolamento (UE 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE		
	regolamento	procedura legislativa ordinaria	data del documento: 23/07/2014 data di entrata in vigore: 17/09/2014 data di applicazione: 1/07/2016, salvo eccezioni
	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)		
	regolamento	procedura legislativa ordinaria	data del documento: 27/04/2016 data di entrata in vigore: 24/05/2016 data di applicazione: 25/05/2018
	Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio		
	direttiva	procedura legislativa ordinaria	data del documento: 27/04/2016 data di entrata in vigore: 24/05/2016 data di recepimento: entro il 25/05/2018
	Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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		
	direttiva	procedura legislativa ordinaria	data del documento: 27/04/2016 data di entrata in vigore: 24/05/2016 data di recepimento: entro il 25/05/2018
	Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione		
	direttiva	procedura legislativa ordinaria	data del documento: 07/06/2016 data di entrata in vigore: 08/08/2016 data di recepimento: entro il 09/05/2018
	Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)		
	proposta di regolamento	procedura legislativa ordinaria (autorità proponenti: Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie)	data del documento: 10/01/2017 data di invio: 10/01/2017; trasmesso al Consiglio data di invio: 10/01/2017; trasmesso al Parlamento

	forma	procedura	termini rilevanti
🔗	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		
	regolamento	procedura legislativa ordinaria	data del documento: 14/11/2018 data di entrata in vigore: 18/12/2018 data di applicazione: 18/06/2019
🔗	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		
	direttiva	procedura legislativa ordinaria	data del documento: 17/04/2019 data di entrata in vigore: 06/06/2019 data di recepimento: entro il 7/6/2021
🔗	Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)		
	regolamento	procedura legislativa ordinaria	data del documento: 17/04/2019 data di entrata in vigore: 27/06/2019 data di applicazione: 27/06/2019, salvo eccezioni
🔗	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 (rifusione)		
	direttiva	procedura legislativa ordinaria	data del documento: 20/06/2019 data di entrata in vigore: 16/07/2019 data di recepimento: entro il 17/07/2021
🔗	Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione		
	proposta di regolamento	procedura legislativa ordinaria (autorità proponenti: Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie)	data del documento: 21/04/2021 data di invio: 21/04/2021; trasmesso al Consiglio data di invio: 21/04/2021; trasmesso al Parlamento
🔗	Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)		
	regolamento	procedura legislativa ordinaria	data del documento: 30/05/2022 data di entrata in vigore: 23/06/2022 data di applicazione: 24/09/2023
🔗	Il Codice di buone pratiche sulla disinformazione rafforzato del 2022		
	linee guida	orientamenti della Commissione europea	pubblicazione: 16/06/2022

	forma	procedura	termini rilevanti
	Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)		
	regolamento	procedura legislativa ordinaria	data del documento: 14/09/2022 data di entrata in vigore: 01/11/2022 data di applicazione: 02/05/2023, salvo eccezioni
	Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020		
	proposta di regolamento	procedura legislativa ordinaria (autorità proponenti: Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie)	data del documento: 15/09/2022 data di invio: 15/09/2022; trasmesso al Consiglio data di invio: 15/09/2022; trasmesso al Parlamento
	Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)		
	regolamento	procedura legislativa ordinaria	data del documento: 19/10/2022 data di entrata in vigore: 17/02/2022 data di applicazione: 17/02/2024, salvo eccezioni
	Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011		
	regolamento	procedura legislativa ordinaria	data del documento: 14/12/2022 data di entrata in vigore: 16/01/2023 data di applicazione: 17/01/2025, salvo eccezioni
	Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)		
	direttiva	procedura legislativa ordinaria	data del documento: 14/12/2022 data di entrata in vigore: 16/01/2023 data di recepimento: entro il 17/10/2024
	Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati)		
	regolamento	procedura legislativa ordinaria	data del documento: 13/12/2023 data di entrata in vigore: 11/01/2024 data di applicazione: entro il 12/09/2025, salvo eccezioni

Riferimenti bibliografici

S. Calzolaio (2017), voce *Protezione dei dati personali*, in "Digesto delle Discipline pubblicistiche", Aggiornamento, Utet Giuridica, 2017

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0123 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Federico Serini

La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana

Il trasferimento di questioni legate alla sovranità degli Stati all'interno di una dimensione sviluppata sugli ideali della a-gerarchia e del libero accesso, quale il cyberspazio, ne sta progressivamente cambiando le sue caratteristiche. Oltre ai tentativi di balcanizzare Internet o di modificarne la sua architettura, un altro tema di attuale interesse riguarda la sicurezza delle infrastrutture informatiche. Questa azione richiede il necessario bilanciamento da parte degli ordinamenti tra l'esigenza di libera circolazione dei beni ICT e la loro sicurezza dal rischio informatico. Il presente contributo intende concentrarsi su quest'ultimo aspetto, ponendo l'attenzione sui c.d. beni ICT posti al crocevia di tali valutazioni e interessi. Dopo aver delineato l'attuale quadro normativo sulla certificazione e standardizzazione di cybersicurezza a livello europeo e nazionale, saranno svolte alcune riflessioni conclusive sulle problematiche e sulle possibili prospettive relative alla sempre maggiore rilevanza della norma tecnica in questo settore.

Cybersecurity Act – Cyber Resilience Act – Procurement beni ICT – Standard e certificati di cybersicurezza

The fragmentation of the merceological cyberspace between certifications and cybersecurity standards. Some considerations in the light of the European and Italian disciplines

The transfer of issues related to the sovereignty of states within a dimension developed on the ideals of a-hierarchy and free access, such as cyberspace, is progressively changing its characteristics. In addition to the attempts to balkanise the Internet or modify its architecture, another issue of current interest concerns the security of information infrastructures This action requires the necessary balancing act on the part of legal systems between the need for free movement of ICT assets and their security from cyber risk. This contribution intends to focus on the latter aspect, focusing on the so-called ICT assets placed at the crossroads of these assessments and interests. After outlining the current legal framework on cybersecurity certification and standardisation on a European and national level, some concluding reflections will be made on the issues and possible perspectives on the increasing relevance of technical standards in this area.

Cybersecurity Act – Cyber Resilience Act – ICT assets procurement – Cybersecurity standards and certificates

L'Autore è dottorando di ricerca in Diritto pubblico, internazionale e comparato presso Sapienza – Università di Roma

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Il cyberspazio come dimensione merceologica: una prospettiva di studio

Spesso confuso o utilizzato come sinonimo di Internet, il cyberspazio rappresenta un concetto complesso e di difficile definizione univoca[1]. La letteratura sul punto, non solo giuridica, è tuttavia concorde nel precisare che le due nozioni non sono sinonimi.

Basti ricordare la definizione di Internet fornita da uno dei creatori della Rete, Vinton Cerf, come «il sistema di trasporto che sposta pacchetti di dati dal punto di origine alla destinazione [ove] diversi protocolli principali costituiscono l'Internet di base. Si tratta dell'*Internet Protocol* – IP, del *Transmission Control Protocol* – TCP e dell'*User Datagram Protocol* – UDP»[2].

Difatti, Internet è il servizio (costituito dalla summenzionata suite di protocolli) che ha permesso alle diverse reti continentali di connettersi tra di loro[3], costituendo lo spazio informazionale che occupa solo una regione del cyberspazio[4], in particolare quella responsabile della trasmissione dei dati e delle informazioni.

Ma ora cerchiamo di capire cosa si intende per cyberspazio. Precisiamo innanzitutto che non si tratta di un concetto giuridico, sebbene ormai diffusamente impiegato all'interno di leggi e regolamenti mediante l'uso del lemma "cyber"[5].

1. Secondo lo studioso F.D. Kramer esistono 28 differenti definizioni del termine *cyberspace*. Cfr. Kramer 2009.
2. Cerf 2022.
3. V. la definizione fornita dall'Enciclopedia Treccani ove l'Internet è definito come la «rete di elaboratori a estensione mondiale, mediante la quale le informazioni contenute in ciascun calcolatore possono essere messe a disposizione di altri utenti che possono accedere alla rete in qualsiasi località del mondo». Sul punto vedi anche Carotti 2016, p. XIII, ove l'A. definisce Internet come «una tecnica di trasmissione di dati».
4. Sul punto si faccia riferimento alla definizione elaborata nel 2022 dal Dipartimento della Difesa statunitense, secondo cui il cyberspazio è un dominio globale all'interno dell'ambiente informativo costituito dalla rete interdipendente di infrastrutture informatiche e di dati residenti «including the internet, telecommunications networks, computer systems, and embedded processors and controllers». Sul punto si rinvia al documento *Defense Primer: Cyberspace Operations* disponibile presso il sito del Congresso USA.
5. Sull'utilizzo del termine "cyberspazio" a livello giuridico si rinvia a Monti 2023a, p. 66, ove l'A. scrive che «invenzioni letterarie come il "ciberspazio" e il suo corollario "virtuale" hanno influenzato negativamente la riflessione giuridica […] essi non sono né fictio juris (come la persona giuridica) né metafore giuridiche (come la nozione di fonti del diritto), necessarie al funzionamento del Sistema. Di conseguenza, pur mantenendo

Come noto, la prima utilizzazione del termine la si trova in un romanzo di un genere letterario che stava prendendo piede negli anni Ottanta del secolo scorso, il *cyberpunk*. In *Neuromancer*, lo scrittore William Gibson ambienta il suo romanzo in una realtà futuristica e distopica ove i personaggi vivono esperienze alternative connettendosi – per l'appunto – al "cyberspace", spazio elettronico a cui è possibile accedere per archiviare, scambiare e trafugare dati e informazioni[6]. Alcuni autori hanno invece descritto il cyberspazio come una «realtà virtuale»[7], altri come una rete internazionale di computer costituente a tutti gli effetti una «electronic frontier»[8].

Con il tempo questa parola venne curiosamente utilizzata in ambiti poco attinenti con la letteratura, ossia a livello politico e militare. Tuttavia, se nel primo caso, come nelle diverse risoluzioni delle Nazioni Unite adottate a partire dal 1998, viene riconosciuta l'esistenza del cyberspazio senza dare definizione e limitandosi solo a definire i comportamenti degli Stati in questo "ambiente"[9]; nell'ambito militare il concetto assume una puntale rappresentazione nella sua struttura e nei suoi caratteri. In questo settore sono state infatti elaborate diverse formulazioni di cyberspazio che lo descrivono, nella gran parte dei casi, attraverso i concetti degli spazi fisici, definendolo quindi come un luogo, o come "dominio"[10].

Il tratto comune alle diverse formulazioni è nella individuazione dei livelli dello spazio cybernetico, anche noti come stratificazioni del cyberspazio. A partire dalla seconda metà degli anni 2000 alcuni studi hanno riorganizzato tali elementi secondo tre macro-livelli quali quello fisico, logico e sociale, di cui:

«a. the human layer: the users of computerization (communications and computers);
b. the logical layer: the software and bits. These move at the speed of light and represent information, instructions, cyberspace assets (such as valuable software, electronic funds), malware (such as Trojan horses), and more;
c. the physical layer: the network physical components, including hardware, mobile infrastructures, and stationary infrastructures, found on

un'indubbia utilità per spiegare fenomeni sociologici, psicologici e anche economici – come appunto, il metaverso – "ciberspazio" e i suoi derivati non dovrebbero avere alcun ruolo nell'individuazione di obiettivi normativi e nella loro trasposizione in leggi e regolamenti». Più diffusamente sul punto v. anche Monti 2023.

6. In particolare, Gibson descriveva il cyberspazio come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione […] Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità, linee di luce allineate nel non-spazio della mente, ammassi di costellazioni di dati» (Gibson 1984, p. 54).
7. L'informatico statunitense Jaron Lanier dà una definizione artistica del cyberspazio, sottolineando le potenzialità intrinseche del mezzo: «A twenty-first century art form that will weave together the three great twentieth-century arts: cinema, jazz and programming», v. Lanier 2017, p. 3.
8. V. Goldsmith-Wu 2006, p. 17 a proposito di John Perry Barlow.
9. Marrani 2020, p. 49 ss.
10. Nel *Warsaw Summit Communiqué* del 9 luglio 2016, l'Organizzazione del Trattato dell'Atlantico del Nord (NATO) ha riconosciuto il cyberspazio «as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea» (art. 70). Allo stesso modo, tempo addietro, nel 2003, la Casa Bianca con il *National Strategy to Secure Cyberspace* definiva lo "spazio cibernetico" come «un sistema nervoso – il sistema di controllo del Paese – composto da centinaia di migliaia di computer interconnessi, server, router, cavi in fibra ottica che permettono alle nostre infrastrutture critiche di lavorare. Così, il sano funzionamento dello spazio cibernetico è essenziale per la nostra economia e la nostra sicurezza nazionale». Nel 2009, Daniel Kuehl, ha definito il cyberspazio come: «un dominio globale nell'ambito dell'ambiente delle informazioni il cui carattere distintivo e unico è caratterizzato dall'uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare e sfruttare le informazioni tramite reti inter-indipendenti e interconnesse che utilizzano le tecnologie dell'informazione e della comunicazione» (Kuehl 2009, pp. 26-28). Lo stesso anno, Martin C. Libicki definisce il cyberspazio individuando tre livelli: fisico, sintattico e semantico: Libicki 2009.

land, at sea, in the air, and in space (henceforth, "the physical spheres")[11]».

Recenti studi, ritenendo ormai obsoleta tale impostazione statica[12], hanno formulato definizioni orientate ad esaltare il profilo dinamico del cyberspazio («la natura dromologica […] dell'ambiente cibernetico»), caratterizzato da due elementi: la velocità di propagazione e l'abbattimento dei confini[13]. Come scrive Luigi Martino, simili caratteristiche «insieme all'economicità dei mezzi, condiziona il rapporto di reciprocità tra territorio, interazioni sociali e dinamiche politiche»[14].

Aderendo a tale tesi, nel presente contributo si propone una scomposizione e reinterpretazione del cyberspazio come insieme di "merci"[15] – per l'appunto cyberspazio "merceologico" – quale realtà in continua espansione in funzione degli sviluppi delle tecnologie informatiche che fanno ingresso nei mercati e che seguono pertanto le relative logiche e regole, tra cui anche i relativi standard di produzione e di qualità.

A tal proposito, intendiamo innanzitutto tracciare una ricostruzione delle "merci" che costituiscono il cyberspazio alla luce della vigente disciplina europea. Partiamo dalla nozione di «rete e sistema informativo», di cui all'art. 6, par. 1, della Direttiva 2022/2555 (ossia la Direttiva NIS II) che la definisce come:

«a. una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972 [ossia come «i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata, e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le

11. Cfr. Even-Siman-tov 2012, p. 10. Analogamente vedi anche la definizione elaborata dal gruppo di esperti indipendenti riuniti nell'International Groups of Experts su invito della NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), in Schmitt 2017, Rule 1-Sovereignty (general principles par. 4, p. 12) «The physical layer comprises the physical network components (i.e. hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consist of the connection that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities». Altra definizione è data dalla norma tecnica ISO/IEC 27032:2012, *Information technology — Security techniques — Guidelines for cybersecurity, Introduction*, che definisce il cyberspazio come quel complesso ambiente risultante dall'interazione di persone, software e servizi su Internet per mezzo di dispositivi tecnologici e reti ad esso connessi, «which does not exist in any physical form».

12. Rattray 2009, pp. 253 ss., ove l'A. scrive che «the "geography" of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or "moved" by insertion of new coded instructions in a router or switch», salvo tuttavia riconoscere che «Cyberspace is not, however, infinitely malleable: limits on the pace and scope of change are governed by physical laws, logical properties of code, and the capacities of organizations and people».

13. Martino 2018, p. 66, ove l'A. scrive che la *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006 ha descritto il cyberspazio attraverso l'acronimo VUCA, ossia: *Volatility*, *Uncertainty*, *Complexity*, *Ambiguity*. Per un tentativo definitorio, secondo sia il profilo statico sia dinamico del cyberspazio, si veda la formulazione elaborata dal gruppo di ricerca istituito presso la Scuola Sant'Anna di Pisa in Mayer-Martino-Mazurier-Tzvetkova 2014.

14. Martino 2018, p. 66.

15. Cfr. Finocchiaro 2001, p. 571, ove l'A. scrive che Internet «non è un luogo ma è un mezzo di comunicazione» che non ha natura unitaria ma è composto da «un insieme di reti e di sottoreti, autonome e senza organizzazione gerarchica».

reti utilizzate per la diffusione radiotelevisiva, e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato»];
b. qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o
c. i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;»[16]

nonché anche i concetti introdotti all'art. 2, nn. 12, 13 e 14 del Regolamento (UE) 2019/881 (anche noto come *Cybersecurity Act*), sul quale si dirà più ampliamente dopo par. 4, relativi a:

«– "prodotto TIC": un elemento o un gruppo di elementi di una rete o di un sistema informativo;
– "servizio TIC": un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;
– "processo TIC": un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC».

La proposta di Regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, anche nota come proposta di *Cyber Resilience Act*, (d'ora in poi anche proposta CRA), definisce invece all'art. 3, n. 1, il "prodotto con elementi digitali" come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente».

Formulazione che riteniamo essere sintesi di quella che era già stata introdotta con la Direttiva 2019/771, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il Regolamento (UE) 2017/2394 e la Direttiva 2009/22/CE, e che abroga la Direttiva 1999/44/CE. All'art. 2, n. 5, lett. b), la Direttiva descrive i "beni con elementi digitali" come «qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni del bene»; mentre ai n. 6 e 7 del medesimo disposto, sono fornite le definizioni di «"contenuto digitale": i dati prodotti e forniti in formato digitale»; «"servizio digitale": a) un servizio che consente al consumatore di creare, trasformare, memorizzare i dati o di accedervi in formato digitale; oppure b) un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore o da altri utenti di tale servizio o qualsiasi altra interazione con tali dati».

Inoltre, dato che i requisiti orizzontali dettati dalla la proposta CRA sono allineati[17] con gli obiettivi dei requisiti delle norme specifiche di cui all'art. 3, par. 3, lett. d), e) ed f) della Direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (c.d. RED), successivamente specificati dal Regolamento delegato (UE) 2022/30[18], riteniamo utile richiamare anche la definizione di "apparecchiature radio" che:

«i) sono di per sé in grado di comunicare tramite Internet, indipendentemente dal fatto che comunichino direttamente o tramite qualsiasi altra apparecchiatura («apparecchiature radio connesse a Internet»), vale a dire che tali apparecchiature connesse a Internet utilizzano protocolli necessari per lo scambio di dati con la rete Internet direttamente o tramite un'apparecchiatura intermedia;
ii) possono essere giocattoli con funzione radio che rientrano anche nell'ambito di applicazione della direttiva 2009/48/CE del Parlamento

16. Riproponiamo qui di seguito anche la definizione del concetto di «rete e sistema informativo» della Direttiva (UE) 2016/1148 (c.d. *Direttiva NIS I*), come «a) una rete di comunicazione elettronica ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE; b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; o c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione».

17 Cfr. considerando 15, della proposta CRA.

18. Chiara 2022.

europeo e del Consiglio oppure sono progettate o destinate esclusivamente alla cura dei bambini, come i monitor per bambini; o

iii) sono progettate o destinate, esclusivamente o non esclusivamente, ad essere indossate, oppure assicurate o appese a qualsiasi parte del corpo umano (compresa la testa, il collo, il tronco, le braccia, le mani, le gambe e i piedi) o a qualsiasi indumento (compresi copricapi, guanti e calzature) indossato da esseri umani, quali apparecchiature radio sotto forma di orologi da polso, anelli, braccialetti, cuffie, auricolari o occhiali («apparecchiature radio indossabili»)».

Alla luce di tali richiami, è possibile intuire, almeno per quanto riguarda l'ordinamento europeo e degli Stati membri, che l'infrastruttura logica e materiale del cyberspazio possa essere interpretata come un agglomerato di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione (d'ora in poi "beni ICT") che circolano nel mercato globale.

In particolare, riteniamo che cyberspazio e mercato liberalizzato rispondano a regole simili[19]. Se per il primo è essenziale garantire il libero flusso delle informazioni per mezzo della tecnica informatica e il funzionamento delle tante infrastrutture che ne consentono la sua esistenza, per il secondo il fine è quello di garantire lo scambio di beni e di servizi che alimenta la circolazione dei beni ICT nei mercati.

L'Unione europea, come emerge dalla *Strategia per il mercato unico digitale*[20], intende coniugare queste due esigenze integrando le dinamiche della concorrenza con l'esigenza di sicurezza dei beni ICT (e dei contenuti digitali), promuovendo un circuito virtuoso che trova fondamento nella certezza giuridica e nella fiducia dei consumatori e dei venditori[21].

Nel presente lavoro si farà riferimento al concetto di cyberspazio "merceologico" al fine di tentare di analizzare gli effetti delle politiche pubbliche, europee e nazionali, su questa dimensione. Nello specifico, l'obiettivo sarà quello di studiare la gestione di tale complessità attraverso i recenti interventi in materia di certificazione e normazione tecnica a livello europeo e nazionale, quali strumenti che, a seconda del loro utilizzo, possono rappresentare o meno un "attrito" al dinamismo del cyberspazio[22].

2. La governance di cybersicurezza tra frammentazione tecnica e politica del cyberspazio

In *Connectography*, Paragh Khanna scrive che «Internet è stata pensata come una struttura a network, il cui obiettivo è quello di connettere tra loro i nodi di questo network, non certo di rappresentare le nazioni che ne fanno parte». Tuttavia preconizza lo studioso, questa rete oggi «sta evolvendosi dallo stato di collettività non statuale e non governata, dotata soltanto di una supervisione tecnica, a quello di arena geopolitica percorsa dai processi di intensa complessità»[23].

Tale situazione è frutto di un processo evolutivo della regolazione del cyberspazio che possiamo

19. Precisiamo tuttavia che non intendiamo assimilare la *lex informatica* alla *lex mercatoria*. Sul punto si rinvia a Finocchiaro 2001, p. 605 ss., ove l'A. svolge una fondamentale distinzione secondo cui «mentre la *lex informatica*, intesa come insieme di regole tecniche che veicolano scelte giuridiche, si applicherebbe ad ogni tipo di relazione, la *lex mercatoria* è, invece, diritto della classe dei mercanti, applicabile ai rapporti tra imprese». Tuttavia, l'espressione *lex mercatoria* non è sempre utilizzata in maniera univoca, questione che ha dato motivo di aprire un dibattito sul suo significato. A tal proposito v. Berger 1999; Galgano 2016; Goldman 1983; Teubner 1996, pp. 3-28; Mertens 1996, p. 31 ss..

20. COM(2015) 192, *Strategia per il mercato unico digitale in Europa*. In particolare, si faccia riferimento al punto 2.3 relativo a "Impedire i geoblocchi ingiustificati", e al punto 3.4 "Aumentare fiducia e sicurezza nei servizi digitali e nella gestione dei dati personali".

21. Cfr. considerando 5, Direttiva 2019/771 relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE.

22. Sul punto si faccia riferimento a Khanna 2016, p. 66 ss., ove l'A. prendendo in prestito dalla fisica i concetti di "flusso" e "attrito" propone uno studio sulla gestione della complessità delle connessioni, riferita non solo ad Internet ma ad ogni forma di interazione tra esseri umani e cose nel mondo.

23. *Ivi*, p. 451 ss.

distinguere in due macro-momenti. I primi decenni dalla creazione di Internet sono stati caratterizzati dall'assenza di vincoli da parte degli Stati. Durante questo periodo, i governi hanno infatti accettato la necessità di un modello di regolamentazione flessibile e favorevole all'innovazione, quale quello della *self-regulation*. Modello che tuttavia da una parte ha dato inizio all'uso commerciale di Internet[24], dall'altra ha segnato il fallimento del movimento libertario della Rete che auspicava la creazione di uno spazio fuori dalla giurisdizione dei poteri dei governi[25].

Nell'ultimo ventennio, la crescente consapevolezza sui rischi della Rete ha tuttavia portato i poteri pubblici a volgere l'attenzione verso il cyberspazio, dimostrando «non solo di [poterlo] regolamentare ma anche "iper-regolare"»[26].

La questione che ci si pone oggi quindi è in che maniera gli Stati, il cui intervento è successivo nel tempo, intendano regolare il cyberspazio, ora inteso come quel complesso di software e hardware che garantiscono la connettività universale grazie al servizio Internet in virtù dei principi di neutralità e libero accesso.

Il dato certo fornito dalla dottrina internazional-pubblicistica è che, mentre uno Stato può invocare la propria sovranità territoriale per regolamentare hardware e utenti che risiedono in esso, nessuno Stato – singolarmente considerato – può pretendere di regolare l'intero spazio informazionale cybernetico[27].

Non esiste neppure un'organizzazione internazionale competente a tal proposito. Anche a seguito delle modifiche alla struttura dell'ICANN volte a garantire l'indipendenza dal governo degli Stati Uniti del sistema di regolamentazione del *Domain Name Server* (DNS), non si è giunti alla conclusione di ritenere tale ente alla stregua di una organizzazione internazionale. Sia perché solo una parte del governo di Internet passa per i meccanismi giuridici che regolano il sistema DNS[28], sia perché, malgrado il tentativo di approdare verso un modello in cui tutte le parti interessate, compresi i governi, partecipino in condizioni di parità[29], gli USA continuano a gestire unilateralmente detto sistema[30].

Come ravvisato da Goldsmith e Wu in tempi recenti, vi sono aspetti delle reti che non possono essere regolati unilateralmente ma necessitano di uno sforzo di regolazione condivisa a livello globale[31]. Tuttavia, allo stato attuale, considerata l'incertezza dei rapporti tra i poteri sovrani e il cyberspazio[32], e nell'assenza di un «founding international constitutional moment»[33], gli Stati

24. Goldsmith-Wu 2006.
25. Barlow 1996.
26. Pollicino 2023, p. 415.
27. Hollis 2014, p. 11.
28. Ruotolo 2014, p. 249.
29. La gestione del sistema DNS è stata sin dalle origini affidata al Governo degli Stati Uniti, il quale tuttavia aveva concepito *ab origine* il proprio ruolo in maniera temporanea, come emerge dallo *Statement of Policy on the Management of Internet Names and Addresses* emanato il 10 giugno 1998 dal Dipartimento del commercio statunitense ove è espresso l'impegno ad una transizione che consenta al settore privato di avere un ruolo dominante nella gestione del DNS. Nel 2003, il *World Summit on Information Society* (WSIS) delle Nazioni Unite aveva studiato i possibili meccanismi idonei a garantire un più ampio coinvolgimento internazionale nella governance di Internet e in particolare nella gestione del sistema dei nomi di dominio, ove nessun governo avrebbe dovuto rivestire un ruolo preminente. Nonché si faccia riferimento anche al *Montevideo Statement on the Future of Internet Cooperation* del 2013 ove le principali organizzazioni responsabili della gestione tecnica di Internet (ICANN, IETF, ISoc) hanno auspicato un'accelerazione della globalizzazione delle funzioni di ICANN e IANA (*Internet Assigned Numbers Authority*, la sezione di ICANN, che concretamente gestisce il DNS). Sul punto più ampiamente si rinvia a Ruotolo 2016, p. 38.
30. *Ibidem*.
31. Goldsmith-Wu 2006, p. 164.
32. Lessig 2006, p. 302.
33. *Ibidem*.

stanno tentando di plasmare Internet e il cyberspazio secondo propri orientamenti ideologici e interpretativi[34].

A dire il vero il tema ha solitamente sollevato preoccupazioni circa la frammentazione di Internet, quale servizio concepito e sviluppato come universale e privo di barriere[35].

Data l'incertezza del termine, la letteratura sul punto ha enucleato tre tipologie di frammentazione: «*Technical Fragmentation*: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points. *Governmental Fragmentation*: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. *Commercial Fragmentation*: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources»[36].

Tali definizioni ci sembrano utili in quanto riteniamo che così come si è soliti parlare della frammentazione di Internet, altra questione di non secondario rilievo è la frammentazione del cyberspazio. Gli standard e le certificazioni di cybersicurezza dei prodotti ICT sono un emblematico esempio in tal senso. Si tratta di strumenti frutto di un processo di normazione privata che, se uniformemente diffusi e utilizzati da tutti i soggetti interessati, possono costituire un utile incentivo alla circolazione dei beni ICT nel mercato ed allo stesso tempo essere portatori di indubbi benefici per la sicurezza delle reti e dei sistemi informatici a livello globale, concorrendo a colmare il vuoto dato dal fallimento del diritto internazionale nella stabilità del cyberspazio[37]. Diversamente, la moltiplicazione di norme tecniche e certificazioni diverse tra loro, se non addirittura incompatibili, ha l'effetto di creare barriere nel mercato[38], nonché di incidere negativamente sulla interoperabilità tecnica e sulla sicurezza dei sistemi[39] dal quale potrebbe derivare una inevitabile frammentazione del cyberspazio.

Anche in questo caso, l'elemento tecnico e quello economico appena evidenziati non prescindono da quello politico. Con il tempo gli standard – apparentemente tecnici e apolitici – hanno infatti mostrato di essere espressione di interessi ed esigenze che non sono più quelle del mondo privato e commerciale, ma degli Stati[40].

Un recente esempio sul punto può essere colto nella proposta avanzata nel settembre 2019 da Huawei, *China Mobile Communications Corporation*, China Unicom, e il Ministero cinese dell'industria e delle tecnologie dell'informazione in seno al *Telecommunication Standardization Advisory Group* (TSAG) dell'ITU circa la creazione di una nuova architettura di rete che possa far fronte ai futuri sviluppi delle tecnologie informatiche[41]. Ritenendo ormai obsoleto l'utilizzo del protocollo IPv6, soprattutto in previsione delle tecnologie quantistiche, Huawei ha infatti proposto lo sviluppo di un nuovo protocollo IP[42], facendone richiesta ai Gruppi di Studio del *Telecommunication Standardization Sector* (ITU-T) *Study Group*.

Le prime opposizioni sono state quelle dell'Olanda e della Gran Bretagna, le quali hanno ravvisato che i protocolli di rete sono stati sviluppati con un approccio *bottom-up* e pertanto tale proposta sarebbe dovuta essere presentata in altra sede

34. Eichensehr (2015), p. 329.

35. Bertola-Quintarelli 2023.

36. Drake-Cerf-Kleinwächter 2016, p. 4. Il contributo nasce dall'esigenza di chiarire l'argomento in questione al fine di facilitare il confronto in seno al *World Economic Forum's Multi-year Future of the Internet Initiative* (FII) dato che il concetto di "frammentazione" non ha univoco significato:«A human rights lawyer, a trade economist and a network engineer might each give the term a special shade of meaning based on their respective priorities and experiences» (p. 11).

37. Katagiri 2021.

38. World Trade Organization 2017.

39. Oddenino 2018, pp. 31-51.

40. Mattli-Büthe 2003, pp. 1-42. Sul punto vedi anche Wouters 2023, pp. 66-84.

41. Chen-Wang-Li-Lou-Jiang-Galis 2020.

42. Sulle caratteristiche del nuovo protocollo proposto si rinvia a Jiang 2019.

come l'*Internet Engineering Task Force* (IETF)[43]. Dello stesso avviso è stata anche l'Unione europea che, oltre a sottolineare l'inopportuna sede della proposta, ha anche evidenziato che non vi sono prove che l'attuale standard IP sia inadeguato rispetto allo sviluppo delle nuove funzionalità Internet[44].

Sebbene la proposta cinese sia stata poi respinta dall'ITU, il caso può essere preso in esame per l'analisi dei modelli e delle strategie di governo della Rete che si stanno delineando. Innanzitutto, diversamente dall'esperienza del WCIT-12[45], precisiamo che la proposta avanzata dalla Cina non ha avuto ad oggetto l'espressa revisione della governance di Internet, ma l'"aggiornamento" (*upgrade* nella documentazione ufficiale) del protocollo IP. Motivo che ha stimolato le censure degli oppositori sull'inadeguata sede della presentazione della proposta. Brevemente si precisa che mentre nell'IETF il processo decisionale è trasparente e aperto a tutte le parti interessate (inclusa l'industria, la società civile e il mondo accademico), l'ITU-T segue un modello multilaterale ove gli Stati membri sono gli unici partecipanti ad avere l'ultima parola sull'approvazione della proposta, o esprimere un voto, quando non c'è consenso[46].

Ma la questione che qui più interessa riguarda l'oggetto della proposta – per l'appunto il nuovo protocollo IP, una norma tecnica quindi – il cui utilizzo delineato nella proposta lascia intendere la natura politica delle norme tecniche e degli enti di normazione che le elaborano. Come è stato osservato da Emily Taylor, Kate Jones e Carolina Caeiro, nel caso di specie, «Standards-setting enables it [China] to build its own ideological tenets into the design and architecture of new technology in ways that until recently were largely beneath the radar of human rights bodies. By leading standardization processes, China is looking to reshape the architecture of the Internet and set the rules that will govern the technologies of the future»[47].

I processi di standardizzazione possono quindi consentire agli Stati di inserire i propri principi ideologici nella progettazione e nella architettura delle nuove tecnologie con modalità inedite[48].

Allo stesso modo, anche l'inserimento dell'obiettivo della «leadership on standards, norms and frameworks in cyberspace» che compone uno dei punti della *Strategia europea di cibersicurezza per il decennio digitale* presentata nel dicembre 2020 è un esempio di tale inedito uso delle norme tecniche[49]. Si apprende dal documento, che «[i]nternational standardisation is increasingly used by third countries to advance their political and ideological agenda, which often does not correspond with the values of the EU», motivo per cui l'Unione si impegna a: «Shaping international standards in

43. Sugli aspetti di dettaglio si rinvia a Wouters 2023, p. 71; nonché a Radu-DeGregorio 2023, p. 15 ss.

44. *Ibidem*.

45. Il riferimento è al *World Conference on International Telecommunications* (WCIT) tenutosi a Dubai nel Dicembre 2012. L'obiettivo dell'incontro era quella di applicare a Internet le condizioni dei servizi di telecomunicazione previsti nelle *International Telecommunication Regulations* (ITRs) elaborate dall'Unione Internazionale delle Telecomunicazioni (ITU), nel 1988 sul principio del «chi trasmette paga». Tuttavia altro argomento dell'incontro è stato il tentativo di revisionare la governance di Internet da parte di Cina, Russia e altri Stati del medio-oriente, il cui intento era quello di affidare la gestione della Rete ad un'organizzazione internazionale di stampo classico al fine di aumentare la rilevanza dei governi nella gestione della Rete. Sul punto si rinvia diffusamente a Ruotolo 2014, p. 545 ss.

46. Wouters 2023, pp. 71 e 72.

47. Caeiro-Jones-Taylor 2023, p. 186, ove gli AA. scrivono che «[s]tandards-setting enables it [China] to build its own ideological tenets into the design and architecture of new technology in ways that until recently were largely beneath the radar of human rights bodies. By leading standardization processes, China is looking to reshape the architecture of the Internet and set the rules that will govern the technologies of the future». Si rinvia al citato contributo soprattutto per riguarda l'analisi dell'impatto della proposta cinese sui diritti umani.

48. Mattli-Büthe 2003.

49. European Commission, *Joint communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18, 16 December 2020.

the areas of emerging technologies and the core internet architecture in line with EU values […] to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical. As part of its upcoming Standardisation Strategy, the EU should define its objectives for international standardisation, and conduct proactive and coordinated outreach to promote these at international level»[50].

Le due questioni attengono a particolari aspetti di governance del cyberspazio che si caratterizza per la contrapposizione di due approcci: quello multilaterale, quale metodo in uso nelle organizzazioni internazionali tradizionali, che prevede la sola partecipazione degli Stati (*state based model*, o *top-down*); e quello di governance *multistakeholder*, o *bottom-up*, che coinvolge anche altri soggetti di non secondaria rilevanza nel processo di regolazione, ossia le rappresentanze della società civile, e gli attori privati[51].

Contrapposizione di assetti che, rileva la dottrina di diritto internazionale dell'economia, si riflette anche nei modelli di formazione degli standard di cybersicurezza, di cui nello specifico: da una parte il modello *top-down*, *government-centred* e dall'altra quello *bottom-up*, *multistakeholder*[52].

Lo Standard *WLAN Authentication and Privacy Infrastructure* (WAPI) sviluppato dalla Cina è un tipico esempio riconducibile al primo modello. Tuttavia, il dato reale testimonia una netta maggioranza di standard di cybersicurezza frutto di processi *bottom-up* e quindi dell'affermazione nel mercato di norme tecniche di natura non cogente (volontaria per l'appunto), elaborate da organismi privati e da cui diversi governi, tra cui anche l'Italia, hanno tratto spunto per regolare con norme giuridiche la propria cybersicurezza interna (*rectius* incorporazione)[53].

È il caso del *Cybersecurity Framework* (CSF) sviluppato dal *National Institute of Standards and Technology* (NIST) degli Stati Uniti per la prima volta nel 2013[54], e il cui ultimo aggiornamento è atteso per il 2024[55]. Si tratta di una norma volontaria volta a migliorare la gestione della cybersecurity per le organizzazioni, sia nel settore pubblico che in quello privato. Come si apprende dal testo dell'*executive order* 13636, *Improving Critical Infrastructure Cybersecurity*, la formulazione del *framework* è avvenuta all'interno di una serie di consultazioni aperte alla partecipazione delle più ampie rappresentazioni del governo, ma anche del mondo imprenditoriale (tra cui anche gli stessi proprietari di infrastrutture critiche), mondo accademico, agenzie di normazione e società civile[56].

Sulla scorta di una breve panoramica sulla governance degli standard di cybersicurezza, il presente contributo si concentrerà sulla disciplina della standardizzazione e certificazione a livello europeo e nazionale. Pertanto nel prosieguo, dopo la presentazione di alcuni concetti introduttivi (par. 3), saranno analizzate la normazione tecnica europea (parr. 3.1, 3.2), avendo modo di soffermarci anche sugli standard e gli organismi di normazione di cybersicurezza a livello europeo (par. 3.3), e il quadro di certificazione europea introdotto con il *Cybersecurity Act* (par. 4), e le relative applicazioni a livello italiano (parr. 4.1 e 4.2). Sarà inoltre analizzata la proposta di regolamento *Cyber Resilience Act* (CRA), alla luce dei recenti dibattiti sorti durante il trilogo tra i co-legislatori europei (par. 5).

3. Brevi cenni su certificazione, normazione tecnica e ordinamento giuridico

Possiamo definire brevemente la normazione tecnica come quella «attività di produzione di norme atte ad individuare le caratteristiche tecniche, merceologiche e qualitative dei prodotti industriali da

50. *Ivi*, p. 20.

51. Raymond-DeNardis 2015, pp. 572–616.

52. Peng 2018, pp. 445-470.

53. Shackelford-Russell-Haut 2016.

54. NIST 2014.

55. Teplinsky 2023.

56. Si rinvia al sito della Casa bianca, alla sezione 6 del documento *Consultative Process*, del 12 febbraio 2013.

immettere sul mercato nonché, più recentemente, dei sistemi e processi industriali e dei servizi»[57].

Per certificazione si intende invece «l'attività di verifica e di accertamento del rispetto delle norme tecniche nei singoli prodotti, sistemi o servizi immessi sul mercato»[58].

La normazione tecnica nasce nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti, generando di conseguenza effetti di c.d. *vendor lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante. Solo a seguito della rivoluzione industriale, e al progressivo sviluppo del tessuto produttivo, la normazione tecnica è passata da essere appannaggio di singole aziende agli enti di normazione privati, con il fine di uniformare la produzione industriale a standard comuni[59].

Passando ora al prodotto del processo di normazione, occorre distinguere i concetti di norma e specifica tecnica. Facendo riferimento al quadro definitorio vigente, dettato dal Regolamento 1025/2012 (vedi *infra* par. 3.2), per "norma tecnica" si intende «una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi»[60]. La "specifica tecnica" è invece «un documento che prescrive i requisiti tecnici che un determinato prodotto, processo, servizio o sistema deve soddisfare […]»[61].

Il medesimo Regolamento ha inoltre introdotto la "norma armonizzata", nozione rientrante nell'ampia categoria delle norme tecniche, intesa come «una norma europea adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione»[62] (di cui si dirà dopo al par. 3.2).

Preme tuttavia precisare che l'ordinamento italiano, con legge 21 giugno 1986, n. 317, dando attuazione alla disciplina europea in materia di normazione e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, oltre alle definizioni di cui sopra, prevede anche il concetto di "regola tecnica" definita come «una specificazione tecnica o altro requisito o una regola relativa ai servizi, comprese le disposizioni amministrative che ad esse si applicano, la cui osservanza è obbligatoria, de iure o de facto, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro dell'Unione europea o in una parte importante di esso, nonché, fatte salve quelle di cui all'articolo 9-*ter*, le disposizioni legislative, regolamentari o amministrative che vietano la fabbricazione, l'importazione, la commercializzazione o l'utilizzo di un prodotto oppure la prestazione o l'utilizzo di un servizio o lo stabilimento come fornitore di servizi […]»[63].

Dal punto di vista giuridico, sebbene prendano il nome di "norme", tali strumenti non hanno natura giuridica in quanto la loro formazione non avviene per mezzo di un processo giuridico-politico, ma attraverso alternative forme di aggregazione di interessi all'interno di soggetti non statuali[64], il cui fine è quello di definire univocamente caratteristiche di prodotti, metodi e processi di produzione, nonché caratteristiche o metodi e criteri di valutazione circa la prestazione di un servizio.

57. Caia-Roversi Monaco 1995, p. 13.

58. *Ibidem*.

59. Andreini 1995, p. 45 ss.

60. Art. 2, n. 1, Regolamento 1025/2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.

61. Art. 2, n. 4, Regolamento 1025/2012.

62. Art. 2, n. 1, lett. c), Regolamento 1025/2012.

63. Art. 1, lett. f, della legge 21 giugno 1986, n. 317, "Disposizioni di attuazione di disciplina europea in materia di normazione europea e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione".

64. Cesarini 1929.

Le norme tecniche costituiscono pertanto un complesso di regole, volontarie e consensuali, non impositive di un obbligo o un dovere, ma unicamente di un onere a carico di quei soggetti privati, solitamente attivi nel mondo dell'industria, o soggetti pubblici, come le amministrazioni, che intendono conformarvisi al fine di adeguare le loro attività, prodotti o servizi ad uno standard univoco riconosciuto a livello internazionale[65].

Gli enti di normazione sono soggetti, spesso di natura privata, responsabili della produzione delle norme tecniche. Operano nel multilivello e, «per motivi essenziali storici», non sono più di tre: uno per il settore elettronico, uno per il settore delle telecomunicazioni e l'altro per tutti gli altri settori[66].

A livello internazionale sono presenti l'*International Organization for Standardization* (ISO), l'*International Electrotechnical Commission* (IEC) e l'*International Telecommunication Union* (ITU). A livello europeo troviamo invece l'*European Committee for Standardization* (CEN), l'*European Committee for Electrotechnical Standardization* (CENELEC) e l'*European Telecommunications Standards Institute* (ETSI). In Italia gli Organismi riconosciuti sono l'Ente Nazionale Italiano di Unificazione (UNI) e il Comitato Elettrotecnico Italiano (CEI).

Tra le normative tecniche e l'ordinamento giuridico sussiste una relazione. La norma tecnica acquista rilevanza per l'ordinamento giuridico ogni qualvolta questa venga "assunta" al suo interno, e tipicamente ciò avviene attraverso gli istituti dell'incorporazione e del rinvio.

Vi è incorporazione quando il contenuto della norma tecnica viene trasposto *sic et sempliciter* all'interno di una fonte giuridica (generalmente primaria e/o secondaria), mentre il rinvio consiste nell'esplicito riferimento ad una norma tecnica puntualmente indicata (rinvio fisso o materiale), oppure nell'utilizzo di clausole generali all'interno di un disposto giuridico, come ad esempio il richiamo "alle migliori tecniche disponibili", "allo stato dell'arte" o piuttosto ai "migliori standard tecnici e di sicurezza", facenti riferimento al rispetto di normative tecniche quali presupposto di una buona pratica (rinvio mobile o formale)[67].

La norma tecnica viene così acquisita all'interno della norma giuridica, e quindi nell'ordinamento, suscitando non pochi interrogativi sulla natura di tale fonte una volta che sia stata incorporata o richiamata.

Relativamente al primo caso, nel dubbio se tale strumento potesse comportare una «tecnicizzazione della norma giuridica a contenuto tecnico o giuridicizzazione della norma tecnica incorporata nella norma giuridica»[68], la dottrina maggioritaria è pacificamente concorde nel ritenere che la norma tecnica venga "giuridicizzata", costituendo parte integrante del disposto giuridico. Diversamente, maggiori difficoltà interpretative sono state ravvisate in relazione alla qualificazione delle norme tecniche oggetto di rinvio, soprattutto se si considera che tali fonti, di natura privata, e protette da diritto d'autore, troverebbero una difficile cognizione e applicazione da parte di quei soggetti che non le abbiano acquistate.

Sul punto, alcuni hanno sostenuto che il «mero richiamo, in un documento ufficiale, del numero, titolo o data di applicazione della normativa» – ossia il rinvio materiale – porti alla «messa in corto circuito del diritto d'autore» poiché la norma tecnica così rinviata acquista rilevanza pubblicistica[69]. Tuttavia, il dubbio sembra persistere relativamente al rinvio mobile, solitamente utilizzato nei casi in cui la legge si limita a dettare la disciplina generale di una materia, per poi lasciare ampio margine ai destinatari circa l'utilizzo delle norme tecniche utili a raggiungere il risultato "al meglio delle buone pratiche".

In conclusione, escluso quest'ultimo caso, in cui la norma tecnica conserva il suo carattere di fonte volontaria non cogente, l'incorporazione e il rinvio fisso trasformano la norma tecnica in un atto giuridico, facendole così assumere la denominazione di "norma tecnica pubblica" o "regola tecnica".

65. Salmoni 2002, p. 150 ss.

66. Andreini-Caia-Elias-Roversi Monaco 1995, p. 32.

67. Greco 1999, p. 37 ss.

68. Salmoni 2002.

69. Gigante 1997, p 313 ss.

Tuttavia, come è stato precisato, il ricorso all'incorporazione e al rinvio non fanno dell'ordinamento tecnico un ordinamento giuridico, poiché i prodotti del primo acquistano forza normativa solo attraverso questo metodo di «selezione volontaria operata per il tramite della legge o di altro atto – fonte dell'ordinamento giuridico», conferendo quindi alla norma tecnica «non la qualificazione di fonte del diritto ma efficacia cogente»[70].

3.1. La normazione tecnica europea

L'esperienza dell'Unione europea nel settore nella normazione tecnica è di particolare interesse ai fini della presente trattazione. L'Unione ha fatto ricorso allo strumento della standardizzazione per facilitare il processo di integrazione del mercato unico, ed allo stesso tempo garantire fini sociali come la tutela dell'ambiente e la sicurezza individuale e collettiva[71].

Si distinguono due momenti che hanno caratterizzato la disciplina sulla standardizzazione europea. Fino alla metà degli anni Ottanta del secolo scorso, l'intervento della allora Comunità aveva come unico obiettivo quello di smantellare gli ostacoli tecnici che si frapponevano al libero scambio intracomunitario, tentando di addivenire ad un'armonizzazione degli standard tecnici nazionali per il tramite di direttive. Questo modello risultò tuttavia fallimentare stante la difficoltà di codificare le specifiche tecniche, nonché per le diverse opposizioni dei rappresentanti delle amministrazioni nazionali nelle votazioni all'unanimità in seno al Consiglio che ebbero l'effetto di allungare oltremodo i tempi di adozione delle norme tecniche rendendone ormai obsoleto il contenuto[72].

Successivamente, nel 1985 venne inaugurato il c.d. "Nuovo approccio" in materia di armonizzazione tecnica e normazione[73]. In questo sistema il legislatore comunitario si limitava a stabilire i requisiti minimi obbligatori di interesse collettivo, solitamente in ambiti come sicurezza, salute, ambiente e protezione dei consumatori, delegando agli enti di normazione l'elaborazione delle specifiche tecniche relative ai diversi settori che venivano poi pubblicate in Gazzetta ufficiale come norme armonizzate.

La Commissione affidava quindi, per mezzo di mandato[74], la produzione delle norme tecniche agli organismi di normazione riconosciuti a livello europeo (CEN, CENELEC ed ETSI) anche noti come *European Standardisation Organisations* (ESOs), i quali avevano il compito di elaborarle entro la cornice dettata dalle stesse istituzioni europee che vigilavano sulla loro conformità. La rinuncia della Commissione ad esercitare in via diretta le attribuzioni di rilevanza tecnica veniva così compensata con l'assolvimento di tre fondamentali compiti, ossia: la determinazione degli obiettivi; il controllo sulla "qualità" dell'attività degli enti di normazione e certificazione; e il controllo eventuale e successivo alla immissione nel mercato[75].

Questa strategia ebbe l'effetto di coniugare l'esigenza di tutelare le libertà economiche con la protezione dai rischi derivanti dallo svolgimento delle attività industriali, realizzando così «una integrazione stabile e permanente della regolazione sociale nella concorrenza, nella prospettiva di una ridefinizione di quest'ultima alla luce del principio dello sviluppo armonioso, equilibrato e sostenibile»[76].

70. Iannuzzi 2018, p. 78 ss.

71. Chiti 2003, p. 4027.

72. Andreini-Caia-Elias-Roversi Monaco 1995, p. 52.

73. Risoluzione 85/C 136/01, 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione.

74. Ancor prima dello "sconfinamento" verso ambiti non riservati alla normazione tecnica vi è la questione della "delega delle competenze normative" a soggetti diversi dai pubblici poteri. Sul punto v. Joerges-Schepel-Vos 1999. V. anche Bartoloni 2021.

75. Vesperini 1995, p. 146.

76. Chiti 2003, p. 4027. Sul passaggio dalla eliminazione delle barriere alla libera circolazione delle merci al perseguimento di interessi sociali, v. anche Joerges 1997, pp. 298-299.

Ad esempio, sono frutto di questo nuovo approccio sulla normazione armonizzata, le direttive sulla sicurezza dei giocattoli, la n. 378 del 1988[77], a cui ha fatto seguito la direttiva 2009/48/Ce, e la direttiva sulla sicurezza generale dei prodotti, la n. 59 del 1992, a cui ha fatto seguito la direttiva 2001/95/Ce. In tutti questi casi il legislatore comunitario è intervenuto con il fine di tutelare i consumatori attraverso un sistema di presunzione di sicurezza del prodotto conforme alle specifiche disposizioni comunitarie o, in mancanza, alla pertinente normativa nazionale.

3.2. Segue. Il Regolamento 1025/2012

Anche la nuova disciplina dettata dal Regolamento 1025/2012 sembra andare nella stessa direzione avviata con l'approccio del 1985[78].

Sebbene il fine della normazione resti quello di promuovere la competitività delle imprese – agevolando la libera circolazione dei beni e dei servizi, l'interoperabilità delle reti, i mezzi di comunicazione, lo sviluppo tecnologico e l'innovazione – dalla lettura dei considerando apprendiamo che tale vantaggio concorrenziale è parte del piano politico dell'Unione per fronteggiare le sfide sociali come «il cambiamento climatico, l'uso sostenibile delle risorse, l'innovazione, l'invecchiamento della popolazione, l'integrazione della persone con disabilità, la protezione dei consumatori, la sicurezza dei lavoratori e le condizioni di lavoro»[79].

In particolare, la realizzazione di detti fini, stabilmente integrati con le esigenze del libero mercato, sembra trovare concreta espressione nelle forme di cooperazione tra la Commissione europea e gli enti di normazione, e nell'enfasi posta sull'ampia partecipazione delle parti interessate[80], quali soggetti che rappresentano la dimensione dell'interesse pubblico nel processo di normazione e aiutano a rendere più accettabili le norme agli utilizzatori[81].

Il Regolamento del 2012 richiama in più occasioni tali forme di "pluralismo" nel processo di formazione degli standard quando prevede che le organizzazioni europee di normazione «incoraggiano e facilitano» la rappresentanza e la partecipazione di tutti i soggetti interessati alle proprie attività di normazione[82], e alle consultazioni per l'adozione del Programma annuale che identifica le priorità strategiche in materia di normazione europea[83].

Emerge pertanto il riconoscimento da parte dell'Unione del valore politico assunto dalla normazione tecnica e del suo impatto sulla società, che rende necessaria la più ampia partecipazione non solo dei soggetti destinatari delle norme tecniche, quali le industrie e i consumatori, ma anche le organizzazioni di rappresentanti di interessi pubblici diffusi[84].

77. Direttiva 88/378/CEE, relativa al ravvicinamento delle legislazioni degli Stati membri concernenti la sicurezza dei giocattoli.
78. Regolamento (UE) 1025/2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.
79. Considerando 19 Regolamento (UE) 1025/2012.
80. Zei 2008, p. 372 ss.
81. Comunicazione della commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo, *Integrazione degli aspetti ambientali nella normazione europea*, COM(2004) 130, del 25 febbraio 2004.
82. Cfr. artt. 5, 7, 10, 11, 13, 20 Regolamento (UE) 1025/2012.
83. Art. 8 Regolamento (UE) 1025/2012, si tratta del c.d. Programma di lavoro annuale dell'Unione per la normazione europea.
84. V. Zei 2008, p. 384 ss. In particolare sul valore politico degli standard, il riferimento è agli *Orientamenti generali per la cooperazione tra il CEN, il CENELEC e l'ETSI e la Commissione e l'Associazione europea di libero scambio*, del 28 marzo 2003, GUUE n. C 091 del 16 aprile 2003, in cui si riconosce che «le norme [tecniche] occupano uno spazio sempre maggiore in nuovi settori politici, quali la sicurezza sul luogo di lavoro, la protezione dei consumatori e dell'ambiente, il trasferimento al mercato dei risultati della ricerca o l'attuazione di reti transeuropee».

Tuttavia, dal quadro disciplinare appena descritto restano fuori le norme tecniche non armonizzate, ossia quelle norme prodotte da enti di normazione non europei e quindi elaborate fuori dai "principi fondatori" europei[85]. Questi standard, aventi natura volontaria e non cogente, costituiscono la maggior parte delle specifiche tecniche impiegate nel settore delle ICT. Già nel 2009, la Commissione europea, nel libro bianco sull'ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione, evidenziava come fossero divenuti sempre più attivi nell'elaborazione di tali norme forum e consorzi specializzati a livello globale, e come la politica comunitaria in tema di normalizzazione non rispecchiasse tale evoluzione[86].

Il tema interessa in particolare i requisiti tecnici nelle procedure di appalto pubblico per l'acquisto di hardware, software e servizi di tecnologia dell'informazione.

Il Regolamento 1025/2012 è intervenuto sul punto all'art. 13, ove è previsto che la Commissione, di propria iniziativa o su proposta di uno Stato membro, può decidere di identificare le specifiche tecniche delle ICT che non sono norme nazionali, europee o internazionali, purché non siano confliggenti con quest'ultime (nello specifico con l'Allegato II al Regolamento), «per consentire l'interoperabilità in materia di appalti pubblici».

La Commissione prende questa decisione previa consultazione della piattaforma multilaterale europea sulla normazione delle ICT, che comprende le organizzazioni europee di normazione, gli Stati membri e i soggetti interessati, e previa consultazione del comitato istituito dalla corrispondente legislazione dell'Unione, laddove esiste, o previe altre forme di consultazione di esperti del settore, qualora tale comitato non esista[87].

Al momento la Commissione ha emanato una serie di decisioni con le quali ha identificato come specificazioni ICT per gli appalti pubblici europei, quelli formati, tra gli altri, dall'IETF, l'*Organization for the Advancement of Structured Information Standards* (OASIS), l'*European Computer Manufacturers Association* (ECMA), e il *World Wide Web Consortium* (W3C)[88].

Per completezza aggiungiamo inoltre che, da ultimo, il Regolamento è stato oggetto di recenti interventi che non ne hanno comportato una totale abrogazione, quanto piuttosto un suo aggiornamento relativamente a particolari aspetti della disciplina generale. Nello specifico, con il Regolamento (UE) 2022/2480, si è provveduto a disciplinare le decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti della normazione europea, mentre con il Regolamento (UE) 2023/988, è stata aggiornata la disciplina della sicurezza generale dei prodotti (GDPSR).

3.3. Gli standard di riferimento di cyberiscurezza e gli Organismi di standardizzazione cyber a livello Ue

Gli standard di riferimento per la certificazione della cybersicurezza sono molteplici e si focalizzano sulla certificazione di prodotti (ad es. ISO/IEC 15408), di sistemi di gestione (ad es. ISO/IEC 27001), di servizi e di processi ICT.

Tuttavia, l'affermazione di tali categorie è stata graduale nel tempo[89]. Le prime norme tecniche sono state quelle volte a regolare i processi produttivi al fine di garantire determinate caratteristiche nei prodotti. Le norme di secondo tipo sono invece intervenute sulla progettazione e sulle caratteristiche prestazionali dei prodotti. Infine, con l'introduzione a livello internazionale della famiglia di norme ISO 9000, si sono aggiunte le norme tecniche di terzo tipo, volte a normare l'intero sistema di produzione attraverso la formulazione dei c.d. sistemi di gestione (nello specifico la ISO 9000 è la norma dei sistemi di gestione per la qualità).

Proprio all'interno di quest'ultima categoria, tra gli anni Ottanta e Novanta del secolo scorso, hanno iniziato a prendere forma le prime normative tecniche sulla sicurezza dei sistemi informativi e servizi informatici (*computer security*), nonché

85. Considerando 31, Regolamento (UE) 1025/2012.

86. Commissione delle comunità europee 2009.

87. Cfr. art. 13, par. 3, Regolamento 1025/2012.

88. Kanevskaia 2023, p. 83 ss.

89. Andreini-Caia-Elias-Roversi Monaco 1995, p. 45 ss.

sulla sicurezza delle informazioni (*information security*)[90]. A tal proposito si faccia riferimento ad alcune definizioni individuate nel bollettino dell'agenzia statunitense competente nella gestione delle tecnologie, il *National Institute of Standards and Technology* (NIST), ove per sicurezza informatica, o *computer security*, si intende «la protezione fornita ad un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione)» (NIST SP 800-14). Mentre la norma ISO/IEC 27000:2018, per sicurezza delle informazioni, o *information security*, fa riferimento alla «preservazione della riservatezza, integrità e disponibilità delle informazioni», in qualsiasi forma esse siano rappresentate (digitale o materiale), o qualunque sia la loro modalità di trasmissione (comunicazione elettronica, corriere ecc.).

Il fine principale di tali normative è quello di preservare le tre proprietà fondamentali delle risorse informatiche e delle informazioni affinché queste possano essere considerate sicure, ossia la riservatezza (*confidentiality*), l'integrità (*integrity*) e la disponibilità (*availability*), spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese).

Nello specifico, la riservatezza (o confidenzialità) è la proprietà per cui tali risorse possono essere accedute solo da chi è stato autorizzato o ne abbia il diritto; l'integrità concerne invece la preservazione della correttezza, coerenza e affidabilità e quindi anche la certezza che il sistema informativo e l'informazione non siano stati alterati o modificati da soggetti non autorizzati; infine, per disponibilità si intende la proprietà secondo cui le risorse informatiche e le informazioni dovranno essere utilizzabili ed accessibili ogni qualvolta il soggetto autorizzato lo richieda.

Sebbene esistano un gran numero di norme internazionali, europee e nazionali utili per la mitigazione dei rischi di cybersicurezza, per completezza aggiungiamo che, oltre alle norme tecniche per la sicurezza informatica e delle informazioni (IT) in particolare a livello europeo sono state recepite quelle della famiglia ISO 2700, vi sono anche le norme della serie EN IEC 62443 per le Tecnologie Operative (OT).

Date le brevi premesse sugli standard di cybersicurezza, possiamo passare agli organismi di normazione. A tal proposito, osserviamo che l'esigenza di cybersicurezza, particolarmente avvertita a livello europeo, ha avuto l'effetto di specializzare le tre ESOs. Innanzitutto nel 2011 è stato istituito il *CEN-CENELEC Focus Group on Cybersecurity* (CSCG), volto ad analizzare gli sviluppi tecnologici al fine di elaborare un insieme di raccomandazioni per la definizione di standard internazionali che assicurino un adeguato livello di equità per le imprese e le autorità pubbliche. Tra le diverse attività, nel 2016 il CSCG ha esaminato i diversi significati e utilizzi della parola "cybersecurity" da parte di vari portatori di interessi in diversi standard e ha finalizzato un documento sulla definizione di tale concetto[91].

Sempre nel 2017 è stato istituito il CEN-CLC/JTC 13 *Cybersecurity and Data protection*, il cui obiettivo principale è trasporre gli standard internazionali rilevanti come standard europei (EN) nel settore delle Tecnologie dell'Informazione (IT)[92]. Mentre il Comitato tecnico CLC/TC 65X *Industrial-process measurement, control and automation* è l'altro principale fornitore di standard correlati alla sicurezza informatica nel settore della Tecnologia Operativa (OT)[93].

L'organismo ETSI, nel 2014, ha istituito l'ETSI TC CYBER[94] che si occupa della sicurezza delle infrastrutture, dei dispositivi, dei servizi e dei protocolli, degli strumenti e delle tecniche di sicurezza, dei consigli sulla sicurezza, dell'orientamento e dei requisiti operativi di sicurezza per utenti, produttori e operatori di reti e infrastrutture

90. Russell-Gangemi 1991. In particolare sulla storia della norma tecnica ISO/IEC 27001, si rinvia a Gallotti 2019, p. 247 ss.

91. CSCG 2017.

92. Per ulteriori informazioni si rinvia al sito ufficiale CEN-CLC/JTC 13 Cybersecurity and Data protection.

93. Si rinvia al sito ufficiale del Comitato tecnico CLC/TC 65X Industrial-process measurement, control and automation.

94. Si rinvia al sito ufficiale dell'ETSI TC CYBER.

4. Il framework europeo di certificazione e valutazione: il *Cybersecurity Act*

Nel settembre del 2017, la Commissione ha introdotto un pacchetto di misure volte a potenziare la cybersicurezza europea con nuove iniziative operanti sotto il triplice profilo della resilienza, deterrenza e difesa (*Cybersecurity Package*)[95]. Dal documento si apprende che tra gli obiettivi diretti allo sviluppo della resilienza europea dai cyberattacchi vi è il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

Come noto l'ENISA è stata istituita con il Regolamento della allora Comunità europea n. 460 del 2004[96] con l'obiettivo di creare «un clima di fiducia grazie alla sua indipendenza, alla qualità della consulenza fornita e delle informazioni diffuse, alla trasparenza delle sue procedure e metodi di funzionamento e alla diligenza nello svolgere i compiti ad essa assegnati», attraverso la stretta collaborazione con gli Stati e il settore privato[97]. L'Agenzia venne inizialmente dotata di un mandato temporaneo, via via esteso con i Regolamenti (UE) n. 1007/2008, n. 580/2011 e n. 526/2013. Tuttavia, con il pacchetto del 2017 è stata proposta una modifica legislativa volta a rafforzare il ruolo dell'ENISA a fronte delle nuove funzioni e responsabilità attribuitele dalla allora Direttiva (UE) 2016/1148 sulla Sicurezza delle Reti e delle Informazioni nel 2016 (Direttiva NIS I), nonché per il perseguimento di attività come la preparazione e organizzazione di esercitazioni annuali di cybersicurezza paneuropee che combinino la risposta a diversi livelli, e lo scambio di informazioni di cybersicurezza a livello tecnico, operativo e strategico in collaborazione con gli organismi competenti degli Stati membri, dell'Ue e di tutti gli attori interessati[98].

In sostanza il piano di riforma, poi concretamente formulato con la proposta del 2017[99], prevedeva che l'ENISA non si limitasse a fornire solo consulenze specialistiche, come prefissato nel 2004, ma che fosse fosse investita anche compiti operativi.

Per quel che qui interessa, l'attribuzione di rilievo è certamente quella relativa all'elaborazione della politica europea sulla certificazione di cybersicurezza dei beni ICT. Si tratta di un tema particolarmente sensibile in quanto avvicina la cybersicurezza alle dinamiche del mercato, nel caso di specie, del mercato unico europeo. Come anticipato, gli standard e le certificazioni sono strumenti che, se accettati e utilizzati da tutti gli operatori del settore, possono uniformare il mercato dettando parametri utili non solo sotto il profilo produttivo ma anche della qualità – e quindi della sicurezza – dei prodotti. Nel pacchetto del 2017 veniva denunciata l'esistenza di diversi schemi di certificazione di sicurezza per i prodotti ICT, di cui alcuni validi solo in determinati Stati membri e non in altri, creando così una frammentazione del mercato.

Precisiamo tuttavia che nel tempo sono stati compiuti sforzi per garantire il reciproco riconoscimento dei certificati all'interno dell'Unione, ma con risultati parziali. Esistono diverse iniziative internazionali, come i *Common Criteria for Information Technology Security Evaluation* (noti come *Common Criteria* o CC) per la valutazione della sicurezza delle tecnologie d'informazione e che costituiscono una norma tecnica internazionale per la valutazione della sicurezza informatica, ossia la ISO 15408[100]. I CC e l'associata Metodologia comune per la valutazione della sicurezza delle tecnologie d'informazione costituiscono la base tecnica per un accordo internazionale, il *Common*

95. Commissione Europea, Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 (anche nota come "Cybersecurity package").
96. Regolamento (EC) 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.
97. Cfr. considerando 11, Regolamento (EC) 460/2004.
98. Relativamente allo scambio di informazioni per il contrasto alle minacce informatiche a livello europeo sia concesso rinviare a Serini 2023.
99. Proposta di Regolamento 2017/0225 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, che abroga il Regolamento (UE) 526/2013, e sulla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, COM/2017/0477 ("Cybersecurity Act").
100. Il riferimento è per l'appunto alla norma tecnica ISO/IEC 15408-1:2022, recentemente aggiornata, che stabilisce i concetti e i principi generali della valutazione della sicurezza IT.

Criteria Recognition Arrangement (CCRA), che garantisce che i certificati basati sui CC siano riconosciuti da tutti i firmatari del CCRA. Vi rientrano diversi Stati, sia membri dell'Unione europea, sia extra-Ue[101]. Tuttavia, nel 2017, solo 13 Stati membri risultavano essere firmatari dell'accordo.

Altre iniziative sono state coltivate dalle autorità di certificazione. È il caso dell'accordo di reciproco riconoscimento dei certificati rilasciati in conformità con l'accordo sulla base dei criteri comuni stipulato da parte del Gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (*Senior Officials Group – Information Systems Security*, SOG-IS)[102]. Si tratta tuttavia di un gruppo che comprende solo 12 Stati membri, più la Norvegia.

Data la fotografia del 2017, l'istituzione di un quadro comune sulla certificazione di tali prodotti è sembrata la risposta ad un'esigenza avvertita da tempo che avrebbe procurato evidenti vantaggi alle imprese, le quali non avrebbero più dovuto espletare processi di certificazione diversi per operare a livello transnazionale, rendendo gli elevati parametri di cybersicurezza una fonte di vantaggio competitivo[103].

La proposta, seppur volta ad innescare un circuito vantaggioso sia per l'economia sia per la sicurezza, non è stata scevra di critiche, soprattutto da parte degli Stati membri. Come si apprende dal documento finale del briefing legislativo del 2019 dal titolo *ENISA and the new Cybersecurity Act*[104], il 27 settembre 2017, il Senato francese ha adottato un parere motivato ove è stata contestata la conformità della proposta al principio di sussidiarietà. Nello specifico l'obiezione ha interessato due punti fondamentali. Il primo relativo alle basi di legittimità, le quali sarebbero dovute essere non solo l'articolo 114 TFUE, ma anche l'articolo 5 TUE concernente le questioni di sicurezza[105]; l'altro invece attinente al rapporto tra la sicurezza europea e le "sicurezze" degli Stati membri. Il Senato ha infatti osservato che «la cooperazione europea in materia di sicurezza informatica deve continuare sulla base della partecipazione degli Stati membri e della fornitura volontaria di informazioni sensibili, anche per quanto riguarda la sicurezza nazionale su cui l'ENISA non può quindi disporre di ulteriori poteri investigativi come previsto nell'articolo 7, punto 5 della proposta di regolamento»[106].

Altre osservazioni sono invece pervenute dal settore industriale, particolarmente interessato alla regolazione delle certificazioni di cybersicurezza. Tra i pareri avanzati dai diversi stakeholder, emergono due orientamenti di quelli a favore della certificazione volontaria, la maggior parte, e di quelli favorevoli alla certificazione obbligatoria per alcune categorie di prodotti.

La versione definitiva del *Cybersecurity Act* è stata adottata con il Regolamento 2019/881 con il quale è stato conferito mandato permanente all'Agenzia a fronte dell'ampliamento delle sue funzioni[107]. Tra queste, l'art. 8 del Regolamento,

101. Nazioni aderenti: Australia, Canada, Francia, Germania, India, Italia, Giappone, Malesia, Paesi Bassi, Nuova Zelanda, Norvegia, Repubblica di Corea del Sud, Singapore, Spagna, Svezia, Turchia, Stati Uniti, Austria, Repubblica Ceca, Danimarca, Etiopia, Finlandia, Grecia, Ungheria, Indonesia, Israele, Pakistan, Polonia, Qatar, Slovacchia, Regno Unito. Maggiori informazioni disponibili sul portale web del CCRA.

102. Per ulteriori informazioni si rinvia al sito ufficiale del Senior Officials Group – Information Systems Security, SOG-IS.

103. In realtà, secondo una fotografia dello stato dell'arte del quadro di certificazioni di cybersicurezza subito dopo l'adozione del *Cybersecurity Act*, i livelli di cybersicurezza dei prodotti ICT assicurati dalla normativa «are found to be largely inadequate in assisting organisations in the European Union internal market with resisting and recovering from cyber threats». Sul punto v. Stewart Ferguson 2022, pp. 51-114.

104. Il documento prodotto all'interno del Briefing EU Legislation in Progress del 2019 dal titolo *ENISA and the new Cybersecurity Act*.

105. Come si apprende dalla proposta di *Cybersecurity Act*, le basi di legittimità a cui si è fatto riferimento sono state, oltre all'art. 114 TFUE, l'art. 26 TFUE sull'instaurazione e funzionamento del mercato interno.

106. Si rinvia a par. 10 del documento *ENISA and the new Cybersecurity Act* di cui in nota 104.

107. Regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il

rubricato "Mercato, certificazione della cibersicurezza e normazione" prevede che l'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cybersicurezza dei beni ICT, attraverso le seguenti attività: a) monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza […], in assenza di norme; b) preparando proposte di sistemi europei di certificazione della cibersicurezza («proposte di sistemi») per prodotti TIC, servizi TIC e processi TIC […]; c) valutando i sistemi europei di certificazione della cibersicurezza adottati […]; d) partecipando a valutazioni inter pares […]; e) assistendo la Commissione nel provvedere alle funzioni di segretariato dell'ECCG […].

Si evince pertanto che l'Agenzia è stata posta al centro del processo di certificazione. Nel medesimo Regolamento sono istituiti anche altri due soggetti che supportano l'azione dell'Agenzia in questo settore. Si tratta del Gruppo dei portatori di interessi per la certificazione della cibersicurezza (art. 22 par. 2) e del Gruppo europeo per la certificazione della cibersicurezza – ECCG (art. 62).

Il Gruppo dei portatori di interessi per la certificazione della cibersicurezza, copresieduto dai rappresentanti della Commissione e dall'ENISA, è costituito da esperti riconosciuti che rappresentano diversi portatori di interessi, selezionati dalla Commissione, a seguito di un invito aperto e trasparente, su proposta dell'ENISA, e garantendo un equilibrio tra i diversi gruppi di portatori di interessi, nonché un opportuno equilibrio geografico e di genere.

L'attività del Gruppo consiste nel fornire consulenza alla Commissione sulle questioni strategiche riguardanti il quadro europeo di certificazione della cibersicurezza (lett. a), nonché, su richiesta, in materia di mercato, certificazione della cibersicurezza e normazione (lett. b); assistere la Commissione nell'elaborazione del programma di lavoro progressivo dell'Unione (lett. c) e formulare il relativo parere su detto programma (lett. d)[108]; in casi urgenti, fornisce consulenza alla Commissione e all'ECCG in merito alla necessità di sistemi di certificazione supplementari non inclusi nel programma di lavoro progressivo dell'Unione (lett. e)[109].

Il Gruppo europeo per la certificazione della cybersicurezza (ECCG), presieduto dalla

Regolamento (UE) n. 526/2013. Si precisa inoltre che con tale atto, il legislatore europeo ha introdotto per la prima volta, in un atto giuridico, all'art. 2, n. 1, il concetto di «cybersicurezza» inteso come «insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

108. Il programma di lavoro progressivo dell'Unione per la certificazione europea della cybersicurezza è disciplinato all'art. 47 del *Cybersecurity Act*. Si tratta dello strumento con il quale sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza. Ai sensi del disposto è previsto che «2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza. 3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC e processi TIC o delle relative categorie è giustificata sulla base di una o più delle seguenti motivazioni: a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC o processi TIC e in particolare in relazione al rischio di frammentazione; b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri; c) la domanda di mercato; d) gli sviluppi nel panorama delle minacce informatiche; e) la richiesta di preparazione di una specifica proposta di sistema da parte del'ECCG. 4. La Commissione tiene nella debita considerazione i pareri in merito al progetto di programma di lavoro progressivo dell'Unione espressi dall'ECCG e dal gruppo dei portatori di interessi per la certificazione della cibersicurezza. 5. Il primo programma di lavoro progressivo dell'Unione è pubblicato entro il 28 giugno 2020. Il programma di lavoro progressivo dell'Unione è aggiornato almeno ogni tre anni e più spesso se necessario».

109. Il disposto fa riferimento agli artt. 47 e 48 del *Cybersecurity Act*. L'art. 48, rubricato "Richiesta di un sistema europeo di certificazione della cibersicurezza" prevede che «1. La Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente sulla base del programma di lavoro progressivo dell'Unione. 2. In casi debitamente giustificati la

Commissione con l'assistenza dell'ENISA, è composto da rappresentanti delle autorità nazionali di certificazione della cybersicurezza o da rappresentanti di altre autorità nazionali competenti. Un membro dell'ECCG non può rappresentare più di due Stati membri. Tuttavia, i portatori di interessi e le parti terze interessate possono essere invitati a presenziare alle riunioni dell'ECCG e a partecipare ai suoi lavori.

Relativamente alle funzioni, l'ECCG svolge il ruolo di consigliere sia verso la Commissione nelle sue attività volte a garantire l'attuazione e l'applicazione del programma di lavoro progressivo dell'Unione, le questioni relative alla politica in materia di certificazione della cibersicurezza, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersicurezza (lett. a), sia verso l'ENISA in relazione alla preparazione di una proposta di predisposizione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza *ex* art. 49 (lett. b) su cui poi esprime un parere (lett. c); chiede all'ENISA di preparare le Richieste di sistemi europei di certificazione *ex* art. 48, par. 2 (lett. d); adotta pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cybersicurezza (lett. e); esamina gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cybersicurezza (lett. f); agevola la cooperazione tra le autorità nazionali di certificazione della cibersicurezza attraverso lo sviluppo della capacità e lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti della certificazione della cybersicurezza (lett. g); sostiene l'attuazione dei meccanismi di valutazione *inter pares* in conformità delle regole fissate da un sistema europeo di certificazione della cybersicurezza (lett. h); agevola l'allineamento dei sistemi europei di certificazione della cybersicurezza alle norme riconosciute a livello internazionale, rivedendo tra l'altro i sistemi europei di certificazione della cybersicurezza esistenti e, ove opportuno, rivolgendo raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale (lett. i).

L'ENISA, con il supporto di tali Gruppi, è quindi il soggetto responsabile del monitoraggio, nonché dell'aggiornamento del sistema europeo di certificazione, definito nel Regolamento come la «serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti ICT, servizi ICT e processi ICT»[110].

Tale sistema è tuttavia istituito all'interno del Quadro europeo di certificazione della cybersicurezza, il cui obiettivo è quello di «stabili[re] i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e [in modo da consentire] di riconoscere e utilizzare i certificati europei di cibersicurezza e le dichiarazioni UE di conformità per i prodotti ICT, i servizi ICT o i processi ICT in tutti gli Stati membri»[111].

L'effetto di tale intervento normativo, da una parte è stato quello di sostituire i sistemi nazionali di certificazione per i beni ICT coperti da quello europeo (per quelli non coperti, il sistema nazionale resta in vigore)[112], dall'altra, ha inciso sull'organizzazione delle autorità nazionali di certificazione.

Innanzitutto, come si apprende dall'art. 58, gli Stati membri devono assicurare che le attività delle autorità nazionali di certificazione relative al

Commissione o l'ECCG può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente non incluso nel programma di lavoro progressivo dell'Unione. Il programma di lavoro progressivo dell'Unione è aggiornato di conseguenza».

110. Cfr. art. 2, n. 9, Regolamento (UE) 2019/881. Si invita inoltre alla lettura combinata con l'art. 54, ove sono delineati gli "Elementi dei sistemi europei di certificazione della cybersicurezza".

111. Cfr. considerando 69, Regolamento (UE) 2019/881.

112. Cfr. art. 57, Regolamento (UE) 2019/881.

rilascio dei certificati siano «rigorosamente separate» dalle attività di vigilanza[113]. Altri profili riguardano invece la collaborazione e cooperazione tra le autorità a livello nazionale, nonché con la Commissione, attraverso lo scambio di informazioni e la redazione di relazioni annuali.

Tra questi adempimenti riteniamo opportuno evidenziare l'obbligo imposto agli Stati membri di informare preventivamente «la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersicurezza», al fine di evitare la frammentazione del mercato interno[114].

Preme evidenziare che le autorità nazionali di certificazione della cybersicurezza sono soggette a una procedura di valutazione *inter pares* di cui all'art. 59 del *Cybersecurity Act*, ossia una valutazione «effettuata sulla base di criteri e procedure di valutazione solidi e trasparenti, in particolare per quanto riguarda i requisiti strutturali, di risorse umane e procedurali, la riservatezza e i reclami» (par. 2). Tale valutazione deve essere svolta da almeno due autorità nazionali di altri Stati membri e dalla Commissione, nonché con l'eventuale partecipazione dell'ENISA, e ha luogo almeno una volta ogni cinque anni (par. 4).

Sono inoltre parte del sistema nazionale di certificazione l'organismo nazionale di accreditamento e gli organi di valutazione della conformità.

Il Regolamento 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti, definisce l'organismo nazionale di accreditamento come l'unico soggetto che, su autorizzazione dello Stato, può certificare che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate (ISO/IEC 17011) e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità[115].

L'art. 2, n. 13 definisce invece gli organi di valutazione della conformità come organismi che svolgono attività di «valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni». Tuttavia, per poter erogare tale servizio, il *Cybersecurity Act* prevede che tali soggetti debbano essere accreditati dall'organismo nazionale di accreditamento, ossia «l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento»[116], qualora rispettino

113. Sulle attività delle Autorità nazionali di certificazione il comma 7 dell'art. 58 prevede che queste «a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti; b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi di tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza; c) fatto salvo l'articolo 60, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento; d) monitorano e vigilano sulle attività degli organismi pubblici di cui all'articolo 56, paragrafo 5; e) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità violino le prescrizioni del presente regolamento; f) trattano i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 53, e svolgono le indagini opportune sull'oggetto di tali reclami e informa».

114. Cfr. art. 58, par. 4, Regolamento (UE) 2019/881.

115. Cfr. art. 2, nn. 10 e 11 Regolamento (UE) 765/2008.

116. Cfr. art. 2, n. 11, del Regolamento (UE) 765/2008.

determinati criteri, e per un periodo massimo di cinque anni rinnovabile.

Ai sensi dall'art. 58 del Regolamento 2019/881, gli organi sono soggetti ai poteri di vigilanza e controllo delle autorità di certificazione nazionale, le quali possono limitare, sospendere o revocare l'autorizzazione qualora tali soggetti si pongano in violazione delle prescrizioni del Regolamento.

Definiti brevemente i profili organizzativi del nuovo sistema di certificazione della cybersicurezza, riteniamo ora possibile concentrarci sulla disciplina del certificato di cybersicurezza europeo.

L'art. 2, n. 11 del *Cybersecurity Act* lo defnisce come «un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto ICT, servizio ICT o processo ICT è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza».

Considerate le istanze degli stakeholder sulla natura di tali strumenti, evidenziamo che il legislatore europeo all'art. 56, par. 2 del Regolamento ha stabilito che la certificazione di cybersicurezza è volontaria, salvo tuttavia quanto «diversamente specificato dal diritto dell'Unione o degli Stati membri». Sul punto prosegue, al par. 3, prevedendo che «La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della ciberiscurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di ciberiscurezza dei … [beni ICT] e migliorare il funzionamento del mercato interno».

Il tratto che riteniamo tuttavia di particolare rilievo ai fini della presente trattazione riguarda quanto articolato all'art. 52 del *Cybersecurity Act*, rubricato "Livelli di affidabilità dei sistemi europei di certificazione della cybersicurezza". Il disposto prevede infatti una gradazione dell'affidabilità dei beni ICT in tre livelli, "di base", "sostanziale" ed "elevato", commisurati al livello di rischio associato al previsto uso del prodotto in questione in termini di probabilità e impatto di un incidente.

Considerato che la sicurezza assoluta è una condizione mai reale, il legislatore europeo ha scelto di parametrare tali livelli di affidabilità in base alle abilità e risorse degli attori malevoli. Difatti, un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "di base" assicurano che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «i rischi di base noti di incidenti e attacchi informatici»[117].

Un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "sostanziale" assicurano invece che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate»[118].

Infine, un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "elevato" assicurano che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative»[119].

Ad ognuno di questi livelli il legislatore fa discendere una diversa disciplina delle attività di valutazione da intraprendere che vanno da «almeno un» riesame della documentazione tecnica, come nel caso dell'affidabilità "di base" al più complesso «riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione», relativo ai prodotti ICT con livello di affidabilità "elevato".

Preme inoltre precisare che tale tripartizione incide anche sull'individuazione dei certificatori e dei valutatori. Relativamente ai primi, l'art. 56 al comma 6 prevede che ove il sistema europeo di certificazione di cybersicurezza richieda un livello di affidabilità "elevato", «il certificato europeo di cybersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cybersicurezza» oppure, da un

117. Cfr. art. 52, par. 5, Regolamento (UE) 2019/881.
118. Cfr. art. 52, par. 6, Regolamento (UE) 2019/881.
119. Cfr. art. 52, par. 7, Regolamento (UE) 2019/881.

organismo di valutazione della conformità ma solo in presenza di determinate condizioni[120].

Inoltre, il comma 4 del medesimo disposto prevede che «in casi debitamente giustificati un sistema europeo di certificazione della cybersicurezza può prevedere che i certificati europei di cybersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico», ossia un'autorità nazionale di certificazione della cybersicurezza, o un organismo pubblico accreditato come organismo di valutazione della conformità.

Tale disposizione è particolarmente indicativa. Come si apprende – "tra le righe" – dal citato Regolamento (UE) 765/2008, non tutti gli Stati membri e mondiali sono dotati di un organismo di certificazione della cybersicurezza governativo. Per alcuni contesti tale attività è perlopiù demandata anche ad organismi di valutazione della conformità di natura per lo più privata.

Per quanto riguarda i valutatori, all'art. 53 del *Cybersecurity Act* è stata introdotta l'autovalutazione della conformità, che consente, per i soli beni ICT che presentano un basso rischio e quindi corrispondenti al livello di affidabilità "di base", di affidare al fabbricante o al fornitore la responsabilità di valutare la conformità di tali beni, rilasciando poi la relativa dichiarazione UE di conformità (par. 2), ma a titolo volontario (par. 4).

4.1. Il quadro italiano. Il controllo sul procurement informatico alla luce della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica

Il controllo sui prodotti ICT in Italia è stato disciplinato all'interno del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito con d.l. 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019 n. 133, e successivamente, dal d.lgs. 3 agosto 2022, n. 123, per quanto riguarda l'adeguamento dell'Italia al sistema di certificazione di cybersicurezza europeo (di cui si dirà al par. 4.2).

Relativamente al primo intervento, si tratta di una disciplina con la quale il legislatore italiano è intervenuto a protezione delle reti e delle risorse informatiche in uso presso le infrastrutture critiche, nonché le pubbliche amministrazioni di rilevanza nazionale, con un approccio sistematico e integrativo della disciplina NIS. Difatti, come è stato osservato, sono parte del PSNC «tutti quegli operatori pubblici o privati, che, seppur non ricompresi nell'ambito di applicazione della Direttiva NIS, risultino comunque essenziali per la sicurezza nazionale italiana […]»[121].

In particolare, l'art. 1 co. 1, del d.l. 21 settembre 2019, n. 105 dispone che l'obiettivo della normativa è di elevare i livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici «delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la 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».

Nel complesso, l'attuazione del PSNC consiste in un articolato programma la cui completa e concreta realizzazione è affidata ad una serie di regolamenti attuativi[122].

Con il decreto del Presidente del Consiglio dei ministri del 30 luglio 2020, n. 131, si è provveduto a definire le modalità e i criteri procedurali di individuazione dei soggetti afferenti al Perimetro,

120. Tali condizioni sono che deve esservi la «a) previa approvazione dell'autorità nazionale di certificazione della cybersicurezza per ogni singolo certificato europeo di cybersicurezza rilasciato da un organismo di valutazione della conformità; o b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cybersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cybersicurezza».

121. Cfr. Mele 2020, p. 186. Nello specifico, confrontando le due citate discipline, il PSNC ricomprende anche quei soggetti attivi nei settori interno, difesa, spazio e aerospazio, telecomunicazioni, economia e finanza, servizi digitali, tecnologie critiche.

122. Per un quadro completo sui diversi provvedimenti che compongono la materia si invita a consultare il sito della Camera dei deputati, all'apposita sezione "Aree tematiche" relativa alla "Sicurezza cibernetica" (ultima consultazione il 12 novembre 2023).

affidando poi tale compito – come per la direttiva NIS – ad alcune amministrazioni centrali dello Stato. Si tratta di disposizioni con cui si sono quindi definiti i confini – o in tal caso i "perimetri" – applicativi della normativa a seconda dell'attività svolta dal soggetto di interesse.

A tal proposito, con l'art. 2 del citato d.P.C.M., si è innanzitutto definito un soggetto, esercente una «funzione essenziale dello Stato»: «laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti»[123], mentre un soggetto pubblico o privato presta un «servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato» laddove ponga in essere: «attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale»[124].

Relativamente alla riconduzione all'interno del Perimetro di diversi soggetti pubblici, pare utile evidenziare che alcuni di tali soggetti, originariamente esclusi all'interno della Direttiva NIS I, sono ora confluiti nell'ambito di applicazione della Direttiva (UE) 2022/2555 (anche nota come Direttiva NIS II). Nello specifico si tratta di soggetti «dell'amministrazione centrale qual[i] definit[i] da uno Stato membro conformemente al diritto nazionale»[125].

In linea generale, declinando ed estendendo gli obblighi di sicurezza contemplati dalla disciplina NIS (il riferimento è alla NIS I), il d.l. n. 105/2019 articola una disciplina che da una parte impone particolari obblighi verso i soggetti afferenti al Perimetro, amministrativamente e penalmente sanzionati, dall'altra contribuisce alla istituzione di organi componenti la nuova architettura nazionale di cybersicurezza per quanto riguarda il controllo sui beni ICT.

Tuttavia, l'aspetto di interesse in questa sede riguarda l'esercizio dei poteri di controllo sui beni ICT: accertamenti che vengono effettuati sia preliminarmente all'acquisto, sia una volta concluso il contratto.

Il d.l. 105/2019 affida l'esecuzione dei test sulle risorse informatiche in uso presso soggetti esercenti funzioni o servizi essenziali per lo Stato, al Centro di Valutazione e Certificazione nazionale (CVCN)[126]. Si tratta di un ente originariamente istituito presso l'Istituto Superiore delle Comunicazioni e Tecnologie Informatiche (ISCTI), del Ministero dello sviluppo economico, ed ora collocato presso l'Agenzia per la Cybersicurezza Nazionale (ACN)[127].

Con il d.P.R. 5 febbraio 2021, n. 54, emanato in attuazione dell'art. 1, comma 6, del d.l. 21 settembre 2019, n. 105, è stata dettagliata la disciplina sul punto. Nello specifico, oltre al CVCN, sono stati introdotti anche i Centri di Valutazione (CV) presso il Ministero dell'interno[128] e del Ministero della difesa (Ce.Va.), nonché i Laboratori accreditati in

123. Art. 2, lett. a), d.P.C.M. 30 luglio 2020, n. 131.

124. Art. 2, lett. b), d.P.C.M. 30 luglio 2020, n. 131.

125. Art. 3, par. 1, lett. d) della Direttiva 2022/2555, che rinvia all'art. 2, par. 2, lett. f), punto i) del medesimo provvedimento.

126. Si rinvia al sito ufficiale del CVCV presso l'Agenzia per la Cybersicurezza Nazionale.

127. Il trasferimento è avvenuto in virtù del d.l. 14 giugno 2021, n. 82 relativo a "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale". Per una disamina del provvedimento v. Parona 2021. Sia inoltre concesso rinviare a Serini 2022.

128. Nello specifico, l'organizzazione del Ministero dell'Interno è stata modificata con il DPR 231/2021 che, tra l'altro, disciplina la nuova Direzione centrale per la polizia scientifica e la sicurezza cibernetica. Mentre con il d.l. 34/2020 (cd. "decreto Rilancio", art. 240) è stata istituita la Direzione generale per lo sviluppo della prevenzione e tutela informatiche presso il Dipartimento della pubblica sicurezza del Ministero dell'interno.

prova (LAP), quali centri indipendenti dai soggetti inclusi nel Perimetro e dai fornitori, quali strutture accreditate dal CVCN conformemente alle procedure contemplate dal decreto del Presidente del Consiglio dei ministri del 18 maggio 2022, n. 92.

Come si apprende dalla lettera dell'art. 2 del d.P.R., con il decreto si sono disciplinate «a) le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del CVCN e dei CV, ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri di cui alla lettera b) del presente comma, fatti salvi i casi di deroga di cui all'articolo 1, comma 6, lettera a), del decreto-legge; b) i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione di cui alla lettera a); c) le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi [rispetto ai soggetti afferenti al PSNC]».

Relativamente al profilo operativo, l'istituzione di tali Centri, frutto dell'esigenza di prevenire e attenuare i rischi derivanti da risorse informatiche vulnerabili, è stata definita da alcuni come un «modello derogatorio di procurement relativamente all'affidamento di forniture di beni, servizi ICT e sistemi […]» il quale ha imposto accurate verifiche tecnico-documentali preliminari, al termine del quale potranno essere disposte specifiche condizioni e test – di corretta implementazione e di intrusione – di hardware e software nel bando di gara e/o nel contratto[129]. L'art. 3 del citato d.P.R. n. 54 del 2021, relativo alla "comunicazione di affidamento" impone infatti ai soggetti afferenti al PSNC di comunicare al CVCN, o ai competenti Centri accreditati, l'intenzione di procedere all'affidamento di forniture di risorse informatiche «prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT di cui all'articolo 1, comma 6, lettera a), del decreto-legge [PSNC], anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza». Mentre il successivo art. 9 prevede che anche «successivamente all'aggiudicazione della gara o della stipula del contratto, [tali soggetti] comunica[no] al CVCN o ai CV, in via telematica, i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto di fornitura»[130].

Comunicato l'affidamento, la procedura di verifica e valutazione, il cui metodo è disciplinato all'art. 4, è articolata nelle seguenti fasi: *verifiche preliminari, individuazione di condizioni e test* (art. 5), ove il CVCN o i CV effettuano verifiche preliminari ed eventualmente richiedono al soggetto incluso nel Perimetro le informazioni necessarie per assicurare la collaborazione ai fini dell'individuazione delle condizioni per il fornitore e della tipologia di test di hardware e di software da eseguire; *preparazione all'esecuzione dei test* (art. 6), il CVCN e i CV verificano, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni; *esecuzione del test* (art. 7), il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel Perimetro e al fornitore che sarà eseguito presso i laboratori del CVCN, dei CV e dei LAP o, se necessario, presso il fornitore o il soggetto incluso nel Perimetro; *esito della valutazione e prescrizioni di utilizzo* (art. 8), ove il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test e lo comunicano al soggetto incluso nel Perimetro e al fornitore.

Qualora il Centro si pronunci (entro 45/60 giorni) in senso negativo, questi potrà imporre ai bandi di gara e ai contratti clausole, anche sospensive o risolutive, volte al rispetto delle condizioni e dei test eventualmente disposti dallo stesso.

Preme precisare che tali atti del procedimento di verifica e valutazione «sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'articolo 1, comma 1, del decreto-legge [PSNC]»[131].

Tra le altre ipotesi, le valutazioni possono infatti costituire un'importante fase preliminare anche per l'attivazione dei poteri speciali da parte del

129. Fiorentino 2020, p. 57.

130. Art. 5, co. 9, d.P.R. 54/2021.

131. Art. 4, d.P.R. 54/2021.

Governo (cc.dd. *golden powers*)[132] sui servizi di comunicazione a banda larga basati sulla tecnologia 5G (art. 3, d.l. 105/2019), il cui esercizio è possibile solo qualora, a seguito delle valutazioni svolte dal Centro, emergano «elementi indicanti fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano». Si precisa inoltre che l'art. 4-*bis* del l. 105/2019 interviene in materia di esercizio di poteri speciali del Governo, nei settori della difesa e sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, disciplinati nel d.l. 15 marzo 2012, n. 21, potenziando e ampliandone il loro campo applicativo[133].

4.2. Segue. Il decreto legislativo 3 agosto 2022, n. 123

L'ordinamento italiano si è adeguato al nuovo quadro europeo di certificazione della cybersicurezza, introdotto dal citato *Cybersecurity Act*, con il d.lgs. 3 agosto 2022, n. 123, con cui il Governo[134] ha dato attuazione alla delega di cui all'art. 18 della legge di delegazione europea 2019-2020 (l. 22 aprile 2021, n. 53).

Più precisamente, il provvedimento ha dato attuazione ad alcune disposizioni del titolo III del Regolamento, concernenti la certificazione della cybersicurezza dei beni ICT.

Innanzitutto, come già avvenuto sulla scorta del d.l. 14 giugno 2021, n. 82, il decreto legislativo ha riconosciuto l'Agenzia per la Cybersicurezza Nazionale (ACN) quale "Autorità Nazionale di Certificazione della Cybersicurezza", di cui all'art. 58 del *Cybersecurity Act*[135]. Si tratta di una attività che prima era di competenza dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) operante presso il Ministero dello sviluppo economico (MISE), ove era stato istituito, con il d.P.C.M. del 30 ottobre 2003, lo Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione a cui sovraintende l'Organismo di Certificazione della Sicurezza Informatica (OCSI), oggi anch'esso trasferito presso l'ACN[136].

In virtù di tale funzione, l'Agenzia ha competenze relative al rilascio dei certificati europei di cybersicurezza, quale attività "rigorosamente distinta" da quella di vigilanza. Tali competenze sono infatti affidate a due distinte divisioni dell'Agenzia[137].

Relativamente all'ultima attività, l'art. 5 del decreto legislativo, stabilisce che l'Agenzia svolge la funzione di vigilanza verso i fornitori e i fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità. Attività che può svolgere anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia, con le autorità di vigilanza degli altri Stati membri, e con le forze dell'ordine (soprattutto in sede ispettiva).

Il disposto prevede inoltre che nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti l'emissione di un certificato non conforme, il certificato è revocato: a) se relativo a livelli di affidabilità "elevati"; b) per il livello di affidabilità "di base" o "sostanziale" nel caso in cui il certificato non conforme sia relativo ad un bene ICT che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale, o servizio di comunicazione elettronica, o alla salute o all'incolumità personale; c) se previsto espressamente dallo specifico sistema europeo di certificazione.

Relativamente al rilascio di certificati, conformemente alla lettera del *Cybersecurity Act*, l'art. 6 del d.lgs. 123/2022 affida all'ACN il rilascio dei certificati di cybersicurezza con livello di affidabilità

132. La valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, strumentale ai fini dell'esercizio dei poteri speciali è disciplinata all'art. 12 del d.P.R. 54/2021, rubricato "Casi particolari".

133. Mele 2020, p. 204 ss.

134. Sulla "Prevalenza dell'attività del Governo nella recezione della regolamentazione tecnica comunitaria" si rinvia a Iannuzzi 2006, p. 13.

135. Cfr. art. 4, d.lgs. n. 123/2022.

136. Sul punto si rinvia al sito ufficiale dell'OCSI presso l'Agenzia per la Cyberiscurezza Nazionale.

137. Sul punto si rinvia al d.P.C.M. 9 dicembre 2021, n. 223, "Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale".

"elevato", tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI). La disciplina nazionale prevede inoltre che l'ACN si può avvalere di esperti o di Laboratori di prova (LAP), abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

Il comma 2 stabilisce che ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità "sostanziale" o "di base" unicamente da parte di un organismo pubblico, l'Agenzia può emettere tali certificati attraverso l'OCSI. Tuttavia, il rilascio può avvenire anche ad opera di altro organismo di valutazione della conformità pubblico, comunque accreditato dall'organismo di accreditamento, monitorato e vigilato dall'Agenzia, e designato dalla stessa, salvo diverse disposizioni dello specifico sistema europeo di certificazione.

Altra funzione, che permette all'Agenzia di vigilare sugli organismi di valutazione, riguarda l'obbligo di cui all'art. 8 del d.lgs. dell'organismo di accreditamento nazionale (ossia Accredia[138]), di comunicare all'ACN ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento.

Infine, l'art. 9 dispone che, in assenza di un sistema europeo di certificazione, l'ACN potrà introdurre sistemi nazionali di certificazione per i beni ICT, previa consultazione dei portatori di interesse. Si ricorda tuttavia che, al fine di evitare la frammentazione del mercato interno dei sistemi di certificazione, in questo caso lo Stato italiano sarà tenuto ad informare la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersecurity.

5. Il *Cyber Resilience Act*. Il quadro dei controlli alla luce del recente trilogo tra i co-legislatori europei

All'istituzione del quadro unico armonizzato di certificazioni di cybersicurezza dei beni ICT, attuato con il *Cybersecurity Act*, ha fatto seguito l'istituzione di un quadro armonizzato di obblighi volti a mettere in cybersicurezza l'intera *supply chain* di produzione dei beni ICT.

Con la proposta di Regolamento relativa ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali che modifica il Regolamento (UE) 2019/1020 (anche nota come *Cyber Resilience Act* – CRA), possiamo dire che l'obiettivo di mettere in sicurezza il mercato unico digitale è in fase di completamento.

La proposta introduce infatti norme per l'immissione sul mercato di prodotti con elementi digitali, intesi come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente»[139], al fine di armonizzare il mercato interno dei beni ICT relativamente ai requisiti di cybersicurezza[140].

Si precisa tuttavia che tale ampio ambito di applicazione non trova efficacia verso i prodotti con elementi digitali disciplinati dal Regolamento (UE) 2017/745, relativo ai dispositivi medici per uso umano e accessori per tali dispositivi, del Regolamento (UE) 2017/746, relativo ai dispositivi medicodiagnostici *in vitro* per uso umano e accessori per tali dispositivi, nonché ai prodotti con elementi digitali che siano stati certificati in conformità del Regolamento 2018/1139, relativo al livello elevato ed uniforme di sicurezza dell'aviazione civile, e ai prodotti a cui si applica il Regolamento (UE) 2019/2144, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli[141].

Nello specifico, la proposta disciplina i requisiti essenziali per la progettazione, lo sviluppo e la fabbricazione dei beni ICT rientranti nel suo campo d'applicazione, e gli obblighi per gli operatori economici relativi a tali beni, ed inoltre prevede norme in materia di vigilanza del mercato e loro relativa applicazione.

138. Sulle attività di Accredia nel contesto della cybersicurezza si invita a consultare la pagina ufficiale relativa agli atti del convegno dal titolo "Come gestire il rischio informatico? Il contributo dell'accreditamento e della certificazione alla cybersecurity nazionale", tenuto il 14 novembre 2022 presso Sapienza, Università di Roma.

139. Cfr. art. 3, par. 1, proposta CRA.

140. Chiara 2023, p. 151 ss., a cui si rinvia per una trattazione dettagliata della proposta CRA.

141. Cfr. art. 2, parr. 2 e 3, proposta CRA.

Per quel che interessa il presente contributo ci concentreremo sui primi aspetti, cercando di analizzare il rapporto tra le classi di rischio dei prodotti e i corrispondenti obblighi che gravano sui fabbricanti, rappresentanti autorizzati, importatori e distributori di prodotti con elementi digitali.

La particolarità della proposta di Regolamento è infatti quella di aver suddiviso i beni ICT in due categorie principali in base ai livelli di rischio formulati dalla Commissione e definiti all'interno degli allegati alla proposta[142]. La prima categoria comprende i prodotti "non critici" predefiniti, ossia hardware e software con un basso livello di criticità (ad esempio, hard disk, assistenti domestici intelligenti o giocattoli connessi).

L'art. 5 prevede che tali prodotti possano essere immessi sul mercato se il bene e i processi messi in atto dal fabbricante per la sua produzione sono conformi ai requisiti essenziali di cui all'allegato I, relativo ai "Requisiti essenziali di cybersicurezza", e «a condizione che siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati in maniera adeguata alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se opportuno, aggiornati»[143].

La seconda categoria include invece i "prodotti critici", disciplinati all'art. 6 ed elencati nell'allegato III. Tale categoria è ulteriormente suddivisa in due sottocategorie, la classe I relativa al "rischio inferiore", ove rientrano i prodotti con elementi digitali critici (ad esempio, reti private virtuali e router)[144] e la classe II per il "rischio elevato", ove troviamo i prodotti con elementi digitali altamente critici (ad esempio, sistemi operativi per computer fissi e telefoni cellulari o contatori intelligenti)[145].

In base al loro livello di rischio, i suddetti prodotti digitali sarebbero soggetti a procedure di valutazione della conformità meno o più stringenti per dimostrare la conformità agli obblighi di cybersicurezza stabiliti nella proposta di Regolamento. Premettiamo tuttavia che, tra i diversi operatori economici interessati dalla disciplina, l'onere di svolgere tale valutazione incombe solo sui fabbricanti di cui all'art. 10, par. 2 della proposta.

Tuttavia, considerato quanto già scritto a proposito dei prodotti "non critici", i fabbricanti di tali beni sono tenuti a dichiarare sotto la propria responsabilità che i dispositivi con elementi digitali da loro prodotti sono conformi a tutti i requisiti di sicurezza di cui all'allegato I (*self-assessment*).

Invece per i prodotti "critici", il processo per dimostrare la conformità varia a seconda della sottocategoria presa in considerazione. Per i prodotti critici di classe I (rischi inferiori), il produttore potrebbe ancora effettuare una valutazione autonoma sotto la propria responsabilità, a condizione che applichi al proprio prodotto gli attuali standard armonizzati di cibersicurezza, ad esempio, sviluppati da organizzazioni europee di normazione o schemi di certificazione di cibersicurezza nell'ambito del *Cybersecurity Act*. In assenza di tali standard e schemi per il prodotto in questione, o se il produttore non ha applicato o ha applicato solo in parte gli standard o gli schemi, il produttore dovrebbe sottoporsi a una valutazione di conformità effettuata da un terzo soggetto, ossia l'organismo di valutazione della conformità. Per i prodotti critici di classe II (rischio elevato), i produttori sarebbero soggetti a una valutazione di conformità di terze parti gestita da un organismo di valutazione della conformità.

Preme precisare che, al fine di facilitare la valutazione della conformità ai requisiti stabiliti, la proposta prevede una presunzione di conformità per i prodotti con elementi digitali che siano conformi alle norme armonizzate che traducono i requisiti essenziali della proposta in specifiche tecniche

142. Nel determinare i livelli di rischio la Commissione tiene conto di una serie di indici come la categoria del prodotto, ed in particolare se tale categoria di prodotti sia utilizzata dai soggetti essenziali di cui alla disciplina NIS, se sia una categoria di prodotti su cui detti soggetti fanno affidamento oppure possa avere un'importanza futura per le attività di tali soggetti, o sia pertinente per la resilienza dell'intera catena di approvvigionamento dei prodotti con elementi digitali contro eventi perturbatori.

143. Cfr. art. 5, proposta CRA.

144. Cfr. art. 3, n. 3, proposta CRA.

145. Cfr. art. 3, n. 4, proposta CRA.

dettagliate e che sono adottate conformemente al già ricordato Regolamento 1025/2012[146].

Altri obblighi che incombono sui fabbricanti riguardano la registrazione della documentazione tecnica e l'attenersi agli obblighi di notifica per le violazioni della cybersicurezza ai sensi dell'art. 11 della proposta (di cui si dirà dopo).

Gli importatori sono invece tenuti a mettere sul mercato solo prodotti digitali conformi ai requisiti essenziali di cybersicurezza e recanti la marcatura CE, mentre i distributori dovrebbero verificare che i prodotti digitali rechino la marcatura CE, ed hanno anche l'obbligo di accertarsi che i produttori e gli importatori abbiano adempiuto ai loro obblighi ai sensi della legge.

Al momento in cui si scrive, il testo della proposta è stato oggetto di discussione tra i co-legislatori europei che hanno raggiunto un accordo politico sul punto all'inizio di dicembre 2023. In attesa dell'approvazione del testo definitivo, per il momento riteniamo d'interesse evidenziare alcuni i punti critici sollevati lungo le fasi dell'iter.

Già durante la fase delle votazioni da parte delle Commissioni[147], il *TIC Council,* l'associazione internazionale che rappresenta aziende indipendenti specializzate in testing, ispezione e certificazione, ha criticato un punto nodale della proposta di Regolamento nella parte relativa alla procedura di valutazione della conformità che, come analizzato, differisce a seconda della classificazione del rischio del prodotto, prevedendo per i prodotti "non critici" una procedura di *self-assessment* da parte del fabbricante. Il gruppo di interesse ha infatti sottolineato che secondo le stime circa il 90% dei beni ICT rientrano in tale categoria, e pertanto gran parte delle responsabilità di cybersicurezza graverebbero proprio sui produttori privati, con il conseguente rischio che possano essere immessi sul mercato una certa quantità di dispositivi rischiosi per i consumatori[148]. Si è pertanto auspicato di includere anche tali beni tra quelli oggetto di controllo da parte delle competenti autorità pubbliche.

La *Computer & Communications Industry Association* (CCIA Europe), associazione dell'industria dei computer e delle comunicazioni, ha invece ritenuto eccessive le procedure di valutazione della conformità per i prodotti digitali, le quali potrebbero ostacolare lo sviluppo di nuove tecnologie e servizi[149].

Altre critiche sono state invece mosse dal mondo accademico. Tra queste, Mira Burri e Zaira Zihlmann, le quali ritengono che l'obiettivo dell'Unione europea di elevarsi a produttore di standard di cybersicurezza a livello globale potrebbe sortire l'effetto contrario, ossia di causare la frammentazione della governance globale dei dati[150].

Da settembre 2023, la proposta è passata all'esame congiunto della Commissione, del Parlamento europeo e del Consiglio (c.d. trilogo)[151]. Secondo quanto riportato dagli organi di stampa[152], tra i punti particolarmente dibattuti vi sono stati l'art. 11 relativo all'obbligo di notifica del produttore, e il campo di applicazione della disciplina.

Relativamente al primo, come si può apprendere dal testo dell'art. 11 par. 1 del progetto di Regolamento: «Il produttore deve notificare all'ENISA, senza ritardo e comunque entro 24 ore dal momento in cui ne viene a conoscenza, ogni vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali. […] L'ENISA deve, senza indugi, a meno di giustificati motivi connessi a rischi cibersicurezza, inoltrare la notifica al CSIRT designato per il coordinamento della divulgazione delle vulnerabilità in conformità con la [Direttiva NIS II], agli Stati membri interessati al momento

146. Cfr. considerando 15 proposta CRA.

147. Sul punto si rinvia al documento di "briefing" legislativo del Parlamento europeo, *EU cyber-resilience act*, del novembre 2023.

148. V. TIC Council 2022.

149. V. CCIA Europe 2022.

150. Burri-Zihlmann 2023.

151. Per maggiori dettagli, si rinvia alla pagina del Parlamento europeo dedicata all'osservatorio legislativo sul *Cyber Resilience Act,* 2022/0272(COD).

152. Per i temi discussi nei vari triloghi, si rinvia agli articoli di Euractiv firmati da Luca Bertuzzi, di cui in particolare: Bertuzzi 2023; Bertuzzi 2023a; Bertuzzi 2023b.

della ricezione e informare l'autorità di sorveglianza del mercato sulla vulnerabilità segnalata».

Le preoccupazioni sorte su questo punto hanno riguardato la nozione di «vulnerabilità attivamente sfruttata», introdotta per la prima volta nell'ordinamento europeo con la proposta CRA e definita come «una vulnerabilità per la quale esistono prove affidabili che l'esecuzione di codice dannoso è stata effettuata da un attore su un sistema senza il permesso del proprietario del sistema»[153]. Questa informazione sulla cybersicurezza è particolarmente sensibile poiché rappresenta una vulnerabilità difficile da sanare entro le ventiquattro ore richieste per la notifica, e quindi la sua divulgazione potrebbe costituire un potenziale pericolo se appresa da attori malevoli che potrebbero sfruttarla nuovamente.

Pertanto, rispetto alla formulazione originale dell'art. 11 della proposta, ove il compito di diffondere tali vulnerabilità era affidato all'ENISA, i governi degli Stati membri, temendo che tali vulnerabilità possano costituire rischi per la sicurezza e gli interessi nazionali, hanno proposto di affidare questa funzione di recepimento delle notifiche ai CSIRT nazionali[154].

L'emendamento ha tuttavia aperto ad un'ulteriore questione, anch'essa particolarmente discussa, riguardo alla possibilità per i CSIRT nazionali di ritardare discrezionalmente la trasmissione di tali informazioni per giustificati motivi di cibersicurezza, che possono includere ragioni di sicurezza nazionale e interesse pubblico, nonché ordine pubblico. Secondo alcuni dietro questa eccezione ci sarebbe l'interesse dagli Stati membri a sfruttare essi stessi le vulnerabilità così notificate ai propri CSIRTs per spiare bersagli per motivi di sicurezza nazionale[155].

Da quanto si apprende dall'ultimo trilogo il 30 novembre 2023[156], sembra che questo problema sia stato bilanciato giungendo a soluzioni restrittive che probabilmente faranno parte del testo finale del CRA[157]. Secondo tali indicazioni, il CSIRT nazionale avrà il potere di limitare la segnalazione se il prodotto coinvolto ha principalmente una penetrazione nel mercato nazionale e non comporta rischi significativi per gli altri paesi dell'UE. Inoltre, le autorità nazionali non saranno obbligate a rendere pubbliche le informazioni che ritengono essenziali per proteggere gli interessi fondamentali della sicurezza. Tuttavia, su proposta del Parlamento europeo, si è ottenuto che l'ENISA riceva comunque alcune informazioni per monitorare possibili rischi sistemici per il mercato unico.

Altro punto dibattuto, e connesso con il precedente, ha interessato il campo di applicazione della proposta rispetto ai fabbricanti. Secondo un documento fatto circolare dopo il trilogo, pare che la Commissione abbia proposto di considerare un produttore avere la sua sede principale nel Paese membro dell'Unione in cui sono prese prevalentemente ("*predominantly*") le decisioni relative alla cybersicurezza dei suoi prodotti con elementi digitali[158]. Nel caso in cui questo criterio non trovi efficacia, la sede principale dovrà essere considerata il Paese dell'Unione in cui l'azienda ha il maggior numero di dipendenti[159].

6. Considerazioni conclusive

Il *Cybersecurity Act* e la proposta di Regolamento *Cyber Resilience Act* si pongono l'obiettivo di rendere "cybersicuro" il mercato interno attraverso l'istituzione di sistemi di certificazione e sicurezza della catena di approvvigionamento dei beni ICT. Mentre le competenti autorità europee, in

153. Art. 3, n. 39, proposta CRA.

154. Le proposte del Consiglio europeo sul CRA possono essere consultate sul sito ufficiale alla pagina *Cyber resilience act: member states agree common position on security requirements for digital products* del 19 luglio 2023.

155. Bertuzzi 2023.

156. Si rinvia alla pagina del Consiglio, *Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products*, del 30 novembre 2023.

157. Bertuzzi 2023b.

158. Parte del documento è stato riportato da Euractiv. Il frammento interessato citato da Bertuzzi 2023 è «[a] manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken».

159. *Ibidem*.

particolare l'ENISA, svolgono un ruolo di supporto e promozione della certificazione europea di cybersicurezza, le autorità nazionali di certificazione sono responsabili della implementazione di tale sistema presso gli Stati membri tramite l'esercizio di poteri di vigilanza e sanzione.

Tuttavia, la questione che qui interessa maggiormente non attiene al sistema di controlli sui beni ICT affidato alla certificazione, ma a ciò che permette a tali beni di essere cybersicuri, ossia lo standard.

Come anticipato, le norme tecniche, nate come strumento privato per migliorare i processi produttivi, si sono rapidamente sviluppate come strumenti di intervento indiretto dei poteri pubblici nell'economia, per fini di interesse pubblico come la tutela ambientale, la qualità dei prodotti e la sicurezza.

In precedenza, relativamente agli standard di cybersicurezza si è fatto riferimento alla contrapposizione di modelli di normazione privata *state-centred/top-down* e *multistakeholder/bottom-up*, ove, per quanto riguarda questi ultimi, si è evidenziata la partecipazione sia delle rappresentanze civili e dell'industria, sia degli Stati.

La normazione europea è organizzata "da" e "per" i soggetti interessati sulla base della rappresentanza nazionale e l'iter di formazione di queste norme segue un processo ispirato ai principi riconosciuti dall'Organizzazione mondiale del commercio (OMC) nel settore della normazione, vale a dire, coerenza, trasparenza, apertura, consenso, applicazione volontaria, indipendenza da interessi particolari ed efficienza (c.d. "principi fondatori")[160].

In particolare, il processo di formazione delle "norme armonizzate" (vedi, *supra*, par. 3), disciplinato all'art. 10 del Regolamento 1025/2012, costituisce un esempio di co-regolazione: la Commissione stabilisce i requisiti relativi al contenuto che lo standard deve avere, l'organismo europeo di normazione, delegato a tal proposito in virtù della richiesta di standardizzare, qualora accetti, è vincolato al rispetto di tali prescrizioni.

Come è stato osservato, le parti interessate, quali ad esempio piccole e medie imprese, associazioni ambientaliste e dei consumatori, parti sociali, non sono direttamente coinvolte nel processo di formazione di tali norme, dato che solo i corpi nazionali hanno diritto di voto e di negoziare nella preparazione e nell'adozione degli standard europei[161]. Tali parti hanno infatti diretta rappresentanza all'interno delle organizzazioni europee di normazione e in quelle nazionali[162].

Tuttavia, come è stato osservato, il *Cybersecurity Act*, anche se fa riferimento a norme europee e internazionali, non è una legislazione che si conforma alla disciplina del Regolamento 1025/2012[163]. Infatti, i requisiti degli schemi di certificazione non sono stati definiti all'interno delle tre ESOs, ma all'interno del Gruppo Consultivo ENISA di cui all'art. 21 del *Cybersecurity Act*, composto da «esperti riconosciuti che rappresentano i pertinenti portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le PMI, gli operatori di servizi essenziali, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati in conformità della direttiva (UE) 2018/1972, delle organizzazioni europee di normazione nonché delle autorità di contrasto e delle autorità di controllo preposte alla protezione dei dati»[164].

A tal proposito, merita evidenziare che nella strategia europea per la standardizzazione *Una strategia dell'UE in materia di normazione. Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale* presentata il 2 febbraio 2022[165], è stato fissato l'obiettivo di favorire l'integrità, l'inclusività e l'accessibilità del sistema europeo di normazione attraverso principi di "buona governance".

160. Il considerando 2, Regolamento 1025/2012.

161. Hofmann 2016, p. 18.

162. *Ibidem*.

163. Kohler 2020, p. 9.

164. Art. 21, Regolamento (UE) 2019/881.

165. Commissione europea, Una strategia dell'UE in materia di normazione. *Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, 2 febbraio 2022, p. 4, COM(2022) 31.

Dal documento si apprende della necessità per l'Unione di «integrare i valori democratici fondamentali e gli interessi dell'UE e i principi ecologici e sociali» all'interno delle norme tecniche, «[a]d esempio, le norme in materia di cybersicurezza o resilienza delle infrastrutture critiche […] caratterizzate da una dimensione strategica», ormai non più limitate a trattare questioni relative alle sole componenti tecniche.

L'impressione pertanto è che l'Unione europea, con i citati interventi in materia di cybersicurezza, stia concentrando maggiore peso sul ruolo delle istituzioni pubbliche europee, piuttostoché, come in questo caso, sugli organismi di normazione di natura privata, al fine di sviluppare un sistema di normazione tecnica che sia rispettoso dei più ampi principi di democrazia e rappresentanza, oltreché dei "valori europei".

Tuttavia se da una parte questo sistema favorisce certamente l'armonizzazione delle norme tecniche a livello europeo tra tutti gli Stati membri, dall'altra, come già prospettato da alcuni[166], l'utilizzo della normazione tecnica come veicolo dei valori europei nel contesto globale potrebbe originare possibili frammentazioni nel settore. L'auspicio pertanto è che, come per il Regolamento generale sulla protezione dei dati personali (GDPR), l'"effetto Bruxelles"[167] delle politiche europee faccia effetto anche in questo caso.

Riferimenti bibliografici

P. Andreini (1995), *La normativa tecnica tra sfera pubblica e sfera privata*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di) (1995), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, il Mulino, 1995

J.P. Barlow (1996), *A Declaration of the Independence of Cyberspace*, 8 February 1996

M.E. Bartoloni (2021), *La regolazione privata nel sistema costituzionale dell'unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione*, in "Osservatorio sulle fonti", 2021, n. 3

K.P. Berger (1999), *The Creeping Codification of the Lex Mercatoria*, Kluwer Law International, 1999

V. Bertola, S. Quintarelli (2023), *Internet fatta a pezzi*, Bollati Boringhieri, 2023

L. Bertuzzi (2023), *EU Commission pitches double reporting of open security loopholes in cybersecurity law*, in "Euractiv", 15 November 2023

L. Bertuzzi (2023a), *EU policymakers prepare to close on cybersecurity law for connected devices*, in "Euractiv", 30 November 2023

L. Bertuzzi (2023b), *EU institutions finalise agreement on cybersecurity law for connected products*, in "Euractiv", 5 December 2023

A. Bradford (2019), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2019

M. Burri, Z. Zihlmann (2023), *The EU Cyber Resilience Act – An Appraisal and Contextualization*, in "Zeitschrift für Europarecht (EuZ)", 2023, n. 2

166. Burri-Zihlmann 2023.

167. Bradford 2019.

C. Caeiro, K. Jones, E. Taylor (2023), *Technical Standards and Human Rights: The Case of New IP*, in C. Sabatini (ed.), "Human Rights in a Changing World Order", Chatham House and Brookings Institution Press, 2023

G. Caia, F.A. Roversi Monaco (1995), *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

B. Carotti (2016), *Il sistema di governo di Internet,* Giuffrè, 2016

CCIA Europe (2022), *New EU Cybersecurity Rules Are Well-intended, but Introduce Unnecessary Red Tape*, 15 September 2022

V.G. Cerf (2022), *Sulla governance di Internet*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale Scientifica, 2022

O.W. Cesarini (1929), *Il diritto dei privati*, Quodlibet, 1929

Z. Chen, C. Wang, G. Li, Z. Lou, S. Jiang, A. Galis (2020), *New IP Framework and Protocol for Future Applications*, University College, 2020

P.G. Chiara (2023), *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in "Rivista italiana di informatica e diritto", 2023, n. 1

P.G. Chiara (2022), *European Union – Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices*, in "European Data Protection Law Review", vol. 8, 2022

E. Chiti (2003), *La normalizzazione*, in S. Cassese (a cura di), "Trattato di diritto amministrativo", vol. IV, 2003

Commissione delle comunità europee (2009), *Libro bianco – Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE – Prospettive*, 3 luglio 2009

CSCG (2017), *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2017

W.J. Drake, V.G. Cerf, W. Kleinwächter (2016), *Internet fragmentation: An overview*, World Economic Forum, 2016

K. Eichensehr (2015), *The Cyber-Law of Nations*, in "The Georgetown Law Journal", vol. 103, 2015

S. Even, D. Siman-tov (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117, 2012

G. Finocchiaro (2001), *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in "Contratto e impresa", 2001, n. 2

L. Fiorentino (2020), *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea, L. Fiorentino (a cura di), "I 'poteri speciali' del Governo nei settori strategici", Editoriale Scientifica, 2020

F. Galgano (2016), *Lex mercatoria*, il Mulino, 2016

C. Gallotti (2019), *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001*, Lulu.com, 2019

W. Gibson (1984), *Neuromancer*, Ace books, 1984

M. Gigante (1997), *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in "Rivista italiana di diritto pubblico comunitario", 1997, n. 2

B. Goldman (1983), *Lex mercatoria*, Kluwer Law International, 1983

J. Goldsmith, T. Wu (2006), *Who controls the Internet? Illusion of a boardless world*, Oxford University Press, 2006

N. Greco (1999), *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, in Aa.Vv., "Crisi del diritto, produzione normativa e democrazia degli interessi", Edistudio, 1999

H.C.H. Hofmann (2016), *A European Regulatory Union – The Role of Agencies and Standards*, in P. Koutrakos, J. Snell (eds.), "Research Handbook on the EU's Internal Market", Elgar Publishing, University of Luxembourg Law Working Paper, 2016, n. 1

D.B. Hollis (2014), *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, in J.D. Ohlin, K. Govern, C. Finkelstein (eds.), "Cyberwar: Law & Ethics for Virtual Conflicts", Oxford University Press, 2014

A. Iannuzzi (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018

A. Iannuzzi (2006), *Caratterizzazioni della normazione tecnica nell'ordinamento italiano. Il campo di analisi e di verifica della materia ambientale*, in "Studi parlamentari e di politica costituzionale", 2006, n. 151-152

S. Jiang (2019), *New IP Networking for Network 2030*, Fifth ITU Workshop on Network 2030, International Telecommunication Union, 2019

C. Joerges (1997), *Scientific expertise in Social Regulation and the European Court of Justice: Legal Frameworks for Denationalized Governance Structures*, in C. Joerges, K.-H. Ladeur, E. Vos (eds.), "Integrating Scientific Expertise into Regulatory Decision-Making. National traditions and European Innovation", Nomos, 1997

C. Joerges, H. Schepel, E. Vos (1999), *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the "New Approach"*, in "EUI Working Paper law", 1999, n. 9

O. Kanevskaia (2023), *The law and practice of global ICT standardization*, Cambridge University Press, 2023

N. Katagiri (2021), *Why international law and norms do little in preventing non-state cyber attacks*, in "Journal of Cybersecurity", vol. 7, 2021, n. 1

P. Khanna (2016), *Connectography. Le mappe del futuro ordine mondiale*, Fazi Editore, 2016

C. Kohler (2020), *The EU Cybersecurity Act and European standards: an introduction to the role of European standardization*, in " International Cybersecurity Law Review", vol. 1, 2020

F.D. Kramer (2009), *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

D.T. Kuehl (2009), *From Cyberspace to Cyber-power: Defining the Problem*, in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

J. Lanier (2017), *Dawn of the New Everything: Encounters with Reality and Virtual Reality*, Henry Holt and Co., 2017

L. Lessig (2006), *Code: Version 2.0*, Basic Books, 2006

M.C. Libicki (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009

D. Marrani (2020), *La cooperazione internazionale per la sicurezza e la stabilità del cyberspace*, Editoriale Scientifica, 2020

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica & Società", 2018, n. 1

W. Mattli, T. Büthe (2003), *Setting International Standards: Technological Rationality or Primacy of Power?*, in "World Politics", vol. 56, 2003, n. 1

M. Mayer, L. Martino, P. Mazurier, G. Tzvetkova (2014), *How would you define cyberspace?*, First Draft Pisa, Experimental online laboratory PhD in Politics, Human Rights and Sustainability, Scuola Superiore Sant'Anna, 19 May 2014

S. Mele (2020), *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano, S. Previti (a cura di), "Il diritto di Internet nell'era digitale", Giuffrè, 2020

H.J. Mertens (1996), *Lex Mercatoria: A Self-applying System Beyond National Law?*, in G. Teubner (ed.), "Global law without state", Dartmouth Publishing, 1996

A. Monti (2023), *Digital rights delusion: humans, machines and the technology of information*, Routlege, 2023

A. Monti (2023a), *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano, G. Scorza (a cura di), "Metaverso: diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini giuridica, 2023

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014

A. Oddenino (2018), *Digital standardization cybersecurity issues and international trade law*, in "Questions of International Law", vol. 5, 2018

L. Parona (2021), *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in "Giornale di diritto amministrativo", 2021, n. 6

S.Y. Peng (2018), *'Private' Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, in "Cornell International Law Journal", vol. 51, 2018, n. 2

O. Pollicino (2023), voce *Potere digitale*, in "Enciclopedia del diritto - Potere e Costituzione", V-2023

R. Radu, G. De Gregorio (2023), *The New Era of Internet Governance Technical Fragmentation and Digital Sovereignty Entanglements*, in F. Cristiano, B. van den Berg (eds.), "Hybridity, conflict, and Global Politics of Cybersecurity", Rowman & Littlefield Publishers, 2023

G.J. Rattray (2009), *An Environmental Approach to Understanding Cyberpower*, in "Cyberpower and National Security", in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

M. Raymond, L. DeNardis (2015), *Multistakeholderism: anatomy of an inchoate global institution*, in "International Theory", vol. 7, 2015, n. 3

G.M. Ruotolo (2016), *Il sistema dei nomi di dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in "Il diritto dell'informazione e dell'informatica", 2016, n. 1

G.M. Ruotolo (2014), *Internet (diritto internazionale),* in "Enciclopedia del diritto – Annali", Giuffrè, 2014

D. Russell, G.T. Gangemi (1991), *Computer security basics*, O'Reilly & Associates, 1991

F. Salmoni (2002), *Le norme tecniche*, Giuffrè, 2002

M.N. Schmitt (2017) (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017

F. Serini (2023), *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in "MediaLaws", 2023, n. 3

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

S.J. Shackelford, S. Russell, J. Haut (2016), *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*, in "UC Davis Business Law Journal", vol. 16, 2016, n. 2

D.D. Stewart Ferguson (2022), *European Cybersecurity Certification Schemes and cybersecurity in the EU internal market*, in "International Cybersecurity Law Review", vol. 3, 2022

M.J. Teplinsky (2023), *A Review of NIST's Draft Cybersecurity Framework 2.0*, in "LawFare", 13 September 2023

G. Teubner (1996), *Global Bukowina: Legal Pluralism in the World-Society*, in G. Teubner (ed.), "Global law without state", Dartmouth Publishing, 1996

TIC Council (2022), *TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act*, September 2022

G. Vesperini (1995), *Il controllo della «sicurezza» e della «qualità» dei prodotti industriali: due modelli e confronto*, in P. Andreini, G. Caia, G. Ellas, F.A. Roversi Monaco (a cura di), "Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

World Trade Organization (2017), *Members debate cyber security and chemicals at technical barriers to trade committee*, 2017

J. Wouters (2023), *Corporations and the Making of Public Standards in International Law. The Case of China in the International Telecommunication Union*, in P. Delimatsis, S. Bijlmakers, M.K. Borowicz (eds.), "The Evolution of Transnational Rule-Makers through Crises", Cambridge University Press, 2023

A. Zei (2008), *Tecnica e diritto tra pubblico e privato*, Giuffrè, 2008

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0121 • articolo sottoposto a peer review • pubblicato in anteprima l'8 gen. 2024

Angela Cossiri

Le campagne di disinformazione nell'arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento

Le campagne di disinformazione orchestrate dall'estero in funzione di strategia politica internazionale costituiscono una nuova, concreta minaccia per le democrazie, sia in ragione della fisiologica maggiore vulnerabilità dei sistemi liberali pluralistici, sia in ragione della capillare pervasività dei new media e delle loro modalità di funzionamento. L'Unione europea ha adottato strumenti di diritto per contrastare questo fenomeno: nel contesto delle sanzioni introdotte a seguito dell'invasione dell'Ucraina, sono state sospese le trasmissioni di canali mediatici riconducibili all'ecosistema della propaganda di guerra russa. La decisione di recente è stata oggetto di una sentenza del Tribunale dell'Ue, che sembra aver indicato alcune coordinate essenziali nel necessario bilanciamento tra il contrasto ai pericoli e i diritti fondamentali.

Diritti fondamentali – Bilanciamento – Campagne di disinformazione – Libertà dei media
Sospensione dell'attività di radiodiffusione

Legal Instruments to Counter Threats of Disinformation Campaigns in War: A Balancing Test

As part of international political strategy, disinformation campaigns orchestrated from abroad pose a new and concrete threat to democracies. This phenomenon can be attributed to the vulnerability of pluralist liberal systems and to the pervasiveness of new media. The European Union has implemented legal measures to address these challenges. For instance, in response to the invasion of Ukraine, it imposed sanctions on media channels linked to the Russian war propaganda ecosystem. A recent ruling by the General Court of the EU analysed the restrictions of broadcasting. The decision identified the necessary balance between fighting security threats and protecting fundamental rights.

Fundamental Rights – Balancing Test – Disinformation Campaigns – Media Freedom – Restriction of Broadcasting

L'Autrice è professore associato di Diritto costituzionale nell'Università di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Nuovi strumenti nell'arsenale di guerra e nuove vulnerabilità

Nell'ultimo decennio, accanto al sistema tradizionale dei mezzi di informazione di massa, si è sviluppato molto rapidamente nella dimensione globale un sistema di *new media* digitali: piattaforme web, nate come strumento di contatto sociale interpersonale, si sono velocemente trasformate in mezzi di informazione su larga scala, dotati di capillare pervasività.

La rilevanza costituzionalistica dei new media, così come la loro dimensione pubblicistica, è stata sottolineata dalla Suprema Corte degli Stati Uniti (ad es., Packingham v. North Carolina, No. 582/2017): i social sono considerati le attuali "piazze" e "strade", nelle quali ciascuno, a bassissimo costo, può diventare, in ragione della selezione algoritmica, un potente oratore e al contempo ricevere illimitate informazioni automaticamente scelte. I social sono dunque l'inedito, formidabile e, in certi casi, primario "luogo pubblico", nel quale oggi si esercita la libertà fondamentale di manifestazione del pensiero.

Per inquadrare nella dimensione costituzionale questi nuovi fenomeni è utile non sottovalutarne la complessità. Da un lato, la velocità della trasmissione dei dati ha una capacità senza precedenti di moltiplicare l'impatto. Dall'altro, i new media possono superare frontiere e barriere linguistiche. Di fronte al social network, inoltre, l'individuo è solo e fruisce dell'informazione promanante dagli altri individui in assenza di intermediazioni. In una arena in cui la produzione dell'informazione è decentrata, il flusso dei dati è costante e quantitativamente enorme. Il vecchio problema della concentrazione dei media è superato da una nuova criticità[1]: la realtà risulta deformata dal rimbombo di commenti e re-post su verità e falsità non accertabili. Il "rumore di fondo" è un inquinamento permanente dell'ambiente e la comunicazione si confonde con l'informazione. Come noto, uno dei fattori di incremento del disordine è la *filter bubble*, conseguente alle decisioni dei *gatekeepers* a seguito di profilazione, un meccanismo problematico, ove il Web condizioni la formazione dell'opinione pubblica. Infatti di rado l'utente entrerà in contatto con punti di vista differenti con cui confrontarsi, a differenza di quanto accadrebbe naturalmente nelle "vie" e nelle "piazze" pubbliche non virtuali e sarà spinto all'interno di una comunità autoreferenziale, che rafforzerà le sue convinzioni. La "camera d'eco" è un fenomeno noto nelle democrazie anche per i politici che ne hanno fatto uso a scopo propagandistico, grazie a reti organizzate di bot e utenti di sostegno, pronti a rilanciare contenuti. Nella sfera politica, il rischio conseguente a questo meccanismo è la polarizzazione delle visioni e la radicalizzazione ideologica.

All'interno di questo quadro hanno fatto irruzione soprattutto recentemente nuovi fenomeni. Le democrazie pluraliste si dimostrano particolarmente vulnerabili rispetto a campagne di disinformazione orchestrate dall'estero in funzione di

1. In seguito alla pandemia da Covid-19, l'OMS ha utilizzato nei suoi documenti ufficiali il neologismo "infodemia", per sottolineare la circolazione di una quantità di informazioni eccessiva per poter essere ordinata e vagliata dalla mente umana con l'accuratezza necessaria ad individuare fonti affidabili e ad orientarsi.

strategia politica internazionale. Alcuni governi non democratici hanno compreso che in un ambiente interconnesso è possibile influenzare le preferenze degli individui, spostandole verso gli interessi di chi divulga propaganda in funzione di destabilizzazione. La disinformazione è diventata così anche uno strumento a basso costo, alternativo a quelli d'uso tradizionale, per cercare di ottenere graduali guadagni di potere sul piano internazionale[2]. Per questa via, le implicazioni della disinformazione raggiungono il piano della sicurezza nazionale e internazionale. La politica di difesa è chiamata a gestire l'inedito conflitto tra l'interesse fondamentale alla libera manifestazione del pensiero e la sicurezza.

La disinformazione è diventato un trend crescente dalla pandemia in avanti. La disvelata fragilità delle democrazie liberali in episodi cruciali, quali la Brexit e l'assalto al Campidoglio dopo l'insuccesso elettorale di Trump, hanno presumibilmente rafforzato l'idea di alcuni governi non democratici di utilizzare il Web per una comunicazione strategica, mirata non soltanto a generare consenso al proprio interno, ma anche a destabilizzare e indebolire i paesi avversari. Attori internazionali da tempo hanno iniziato a diffondere campagne organizzate di disinformazione, attraverso un ecosistema di media, ma anche siti fake di *fact-checking*, che ripropongono la narrazione propagandistica, contrastando l'informazione con lo stesso linguaggio utilizzato per contrastare le fake news[3].

2. Gli strumenti di contrasto nella dimensione europea: la sospensione del broadcasting

Di fronte a minacce esterne, gli interessi delle democrazie europee coincidono e, anzi, sono indissolubilmente legati. Inoltre i singoli Stati difficilmente potrebbero fronteggiare sfide così sofisticate e di impatto generale da soli. Non stupisce dunque che la risposta politica e giuridica si collochi anzitutto nella dimensione europea.

L'obiettivo della pace viene perseguito dall'Ue utilizzando differenti strumenti: tra essi, gli aiuti umanitari, la cooperazione allo sviluppo, l'azione per il clima, la politica commerciale. La "Politica estera e di sicurezza comune" (PESC) è la competenza attraverso la quale l'Ue gestisce le relazioni internazionali: secondo l'art. 21.1 TUE, «l'azione dell'Unione sulla scena internazionale si fonda sui principi che ne hanno informato la creazione, lo sviluppo e l'allargamento e che essa si prefigge di promuovere nel resto del mondo: democrazia, Stato di diritto, universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, rispetto della dignità umana, principi di uguaglianza e di solidarietà e rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale. L'Unione […] promuove soluzioni multilaterali ai problemi comuni, in particolare nell'ambito delle Nazioni Unite». In questo settore di competenza, i processi decisionali sono sensibilmente diversi da quelli che si applicano nella maggior parte delle altre competenze. Il Consiglio europeo fissa indirizzi generali poi messi in opera dal Consiglio dei ministri attraverso azioni e posizioni comuni, generalmente decise all'unanimità, secondo il metodo intergovernativo. La legittimazione democratica, così come la *rule of law*, sono piuttosto limitate: circoscritti sono i ruoli giocati in questo settore dal Parlamento europeo e dalla Corte di giustizia[4]. Come nella logica della cooperazione internazionale, la legittimazione è quella propria degli esecutivi degli Stati membri. Tuttavia, da questi terreni passa sempre più la regolazione della sfera pubblica, con un significativo impatto diretto e indiretto su diritti fondamentali civili e politici. Un deficit di legittimazione rappresentativa, per cui sono solo le maggioranze di governo a decidere, è

2. Cfr. Moral 2022.
3. Per fare un esempio, l'invasione armata dell'Ucraina da parte della Federazione russa è stata preceduta, a partire da novembre 2021, da un incremento esponenziale anomalo – da parte dei media sotto controllo presidenziale – dell'uso di parole chiave come "genocidio" e "nazi", come rilevato dalle task force diplomatiche Ue. Cfr. Tyushka 2022.
4. L'art. 275, secondo comma, TFUE, prevede che la Corte è competente solo a controllare il rispetto dell'art. 40 TUE (che "presidia" il confine tra le competenze PESC e non-PESC) e la legittimità delle decisioni PESC che prevedono misure restrittive nei confronti di persone fisiche o giuridiche. Per le limitate competenze n via pregiudiziale, si veda la sentenza della Corte di giustizia (Grande sezione) del 28 marzo 2017, Rosneft, ECLI:EU:C:2017:236.

non solo un vulnus democratico, ma anche e soprattutto un punto di debolezza di politiche sempre più centrali. I procedimenti richiederebbero un ripensamento, affinché le decisioni, destinate a condizionare lo "spazio" comune virtuale poggino su solide basi di legittimazione e consenso popolare. Anche da questo punto di vista, sembra dunque affermarsi la necessità di costruire un'Unione europea più politica di quella emergente dall'attuale disegno istituzionale.

In questo quadro, ci sono vari strumenti di particolare interesse in ordine ai problemi sopra evidenziati. Ad esempio, la cooperazione europea in materia di cyber-security ha lo scopo di contrastare le minacce informatiche, prevenire, scoraggiare e rispondere agli attacchi. La strategia contro la disinformazione intende avversare il fenomeno di "manipolazione e interferenza" promanante dall'estero, consistente in comportamenti per lo più non illegali, che minacciano o hanno il potenziale per produrre un impatto negativo su valori, procedure e processi politici interni alle democrazie europee. A seguito dell'invasione armata dell'Ucraina, gli Stati membri dell'Ue hanno reagito adottando tutti i tipi di misure restrittive a disposizione: economiche, finanziarie, settoriali e individuali[5]. Nonostante il previsto voto unanime all'interno del Consiglio dell'Ue, le decisioni Ue assunte sono state rapide e incisive per il convergere coeso degli Stati membri dell'Unione, salvo qualche iniziale esitazione.

Tra queste sanzioni, il 1° marzo 2022, Il Consiglio dell'Unione, su proposta dell'Alto rappresentante per gli Affari esteri, per la prima volta ha adottato restrizioni consistenti nella sospensione della trasmissione del quotidiano online Sputnik e dell'emittente televisiva statale Russia Today (v. Decisione Pesc 2022/351 del Consiglio[6]), al fine di contrastare le attività di disinformazione nei confronti della società civile degli Stati membri e dei paesi limitrofi.

I considerando dell'atto richiamano anzitutto le conclusioni del 10 maggio 2021 del Consiglio, in cui si è sottolineata la necessità di rafforzare la resilienza dell'Unione e degli Stati membri «nonché la loro capacità di contrastare le minacce ibride, compresa la disinformazione, garantendo l'uso coordinato e integrato degli strumenti esistenti e di eventuali nuovi strumenti». Tali strumenti possono comprendere anche misure preventive su attori statali e non statali ostili. La Federazione russa è riconosciuta la regista di «una sistematica campagna internazionale di manipolazione dei media e di distorsione dei fatti, nell'intento di rafforzare la sua strategia di destabilizzazione dei paesi limitrofi e dell'Unione e dei suoi Stati membri. In particolare la propaganda ha preso di mira, ripetutamente e costantemente, i partiti politici europei, soprattutto durante i periodi elettorali, la società civile, i richiedenti asilo, le minoranze etniche russe, le minoranze di genere, e il funzionamento delle istituzioni democratiche nell'Unione e nei suoi Stati membri». Con riferimento all'aggressione nei confronti dell'Ucraina, la Federazione russa porta avanti da tempo la pratica di lanciare iniziative continue e concertate di propaganda, distorcendo e manipolando la realtà dei fatti. Vari organi di informazione, «sotto lo stabile controllo diretto o indiretto della leadership della Federazione russa» svolgono un ruolo essenziale di cassa di risonanza per tale propaganda di Stato e la loro azione rappresenta «una minaccia consistente e diretta all'ordine pubblico e alla sicurezza dell'Unione».

In ordine alla proporzionalità, la motivazione fa riferimento alla gravità della situazione e alle azioni della Russia che destabilizzano la situazione in Ucraina rendendo "necessario, coerentemente con i diritti e le libertà fondamentali riconosciuti nella Carta dei diritti fondamentali, in particolare con il diritto alla libertà di espressione e di informazione come riconosciuto dall'articolo 11 della stessa, introdurre ulteriori misure restrittive al fine di sospendere urgentemente le attività di radiodiffusione di detti organi di informazione nell'Unione o diretti all'Unione. Tali misure dovrebbero essere mantenute fino a quando l'aggressione nei confronti dell'Ucraina non sarà cessata e fino a quando la Federazione russa e gli organi di informazione ad essa associati non avranno cessato di condurre azioni di propaganda contro l'Unione e i suoi Stati membri. Coerentemente con i diritti e le libertà fondamentali riconosciuti nella Carta dei diritti fondamentali, in particolare con il diritto alla

5. Poli 2022.
6. Decisione (PESC) 2022/351 del Consiglio del 1° marzo 2022 che modifica la decisione 2014/512/PESC concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina e relativo comunicato stampa.

libertà di espressione e di informazione, la libertà d'impresa e il diritto di proprietà sanciti dagli articoli 11, 16 e 17 della stessa, le presenti misure non impediscono a tali organi di stampa e al loro personale di svolgere nell'Unione altre attività oltre alla radiodiffusione, come la ricerca e le interviste. In particolare, le presenti misure non modificano l'obbligo di rispettare i diritti, le libertà e i principi di cui all'articolo 6 del trattato sull'Unione europea, compresa la Carta dei diritti fondamentali dell'Unione europea, e di cui alle costituzioni degli Stati membri, nei rispettivi ambiti di applicazione".

La decisione introduce una modifica alla decisione 2014/512/PESC: l'obiettivo della sospensione viene raggiunto introducendo un divieto agli operatori circa «la radiodiffusione, ovvero il conferimento della capacità di diffondere, l'agevolazione della radiodiffusione o altro concorso a tal fine, dei contenuti delle persone giuridiche, delle entità o degli organismi elencati nell'allegato IX [Sputnik e Russia Today], anche sotto forma di trasmissione o distribuzione tramite mezzi quali cavo, satellite, IP-TV, fornitori di servizi internet, piattaforma o applicazione di condivisione di video su internet, siano essi nuovi o preinstallati. Sono sospesi qualsiasi licenza o autorizzazione di radiodiffusione e qualsiasi accordo di trasmissione e distribuzione»[7].

3. L'impugnazione e la sentenza del Tribunale UE

L'8 marzo 2022 uno dei destinatari della decisione (PESC) 2022/351 del Consiglio, RT France, ne ha chiesto l'annullamento, unitamente alla richiesta di annullamento del regolamento (UE) 2022/350 del Consiglio, sempre del 1° marzo 2022, che modifica il regolamento (UE) n. 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina. Il ricorrente lamenta la violazione dei diritti della difesa, della libertà di espressione e di informazione, della libertà d'impresa e del principio di non discriminazione in base alla nazionalità; inoltre, contesta la competenza del Consiglio ad adottare gli atti impugnati. Il Tribunale Ue, dopo aver rigettato la domanda di provvedimenti provvisori, respinge anche il ricorso con la sentenza del 27 luglio 2022[8], pronunciata dalla Grande Sezione[9].

3.1. La questione della competenza

Le argomentazioni addotte circa la questione della competenza sono significative per la perimetrazione della competenza in materia di politica estera e sicurezza comune, che appare capace di assorbire altre competenze di livello nazionale, almeno nelle circostanze eccezionali in cui il caso si colloca. Il Tribunale inizia su questo punto il suo ragionamento, esaminando la correttezza della base giuridica indicata nell'atto: l'art. 29 TUE conferisce al Consiglio il potere di «adotta[re] decisioni che definiscono la posizione dell'Unione su una questione particolare di natura geografica o tematica». Il Tribunale, adeguandosi a precedenti, ritiene che la nozione di "posizione dell'Unione" si presti ad un'interpretazione ampia, di modo che possono essere adottati sul fondamento di tale articolo non solo atti aventi carattere programmatico, ma anche decisioni che prevedano misure atte a modificare direttamente la situazione giuridica di singoli, come confermato dall'articolo 275, c. 2, TFUE (par. 51 della sentenza). Se il Consiglio dispone di un ampio margine nel definire l'oggetto delle misure restrittive adottate dall'Unione nel settore della PESC, esso ha correttamente considerato che, di fronte alla crisi internazionale causata dall'aggressione dell'Ucraina, le

7. Alla decisione in questione segue un importante passaggio. Il 27 ottobre 2022 è stato pubblicato nella Gazzetta ufficiale dell'Unione europea il regolamento (UE) 2022/2065 del Parlamento e del Consiglio del 19 ottobre relativo a un mercato unico dei servizi digitali. L'atto modifica, senza sostituirla, la risalente direttiva 2000/31/CE introduttiva della regolazione dei servizi digitali. L'accordo politico in Consiglio dell'Unione matura proprio il 14 marzo 2022, in un contesto senz'altro definibile emergenziale. Infatti, dopo una crisi diplomatica internazionale di alcune settimane, la formale sospensione delle ostilità tra Russia e Ucraina, che durava dal 2015, viene interrotta il 22 febbraio dall'invasione armata dell'Ucraina. Il conflitto, informano le strutture diplomatiche e di *intelligence*, oltre ad essere stato preceduto da movimentazioni di truppe nella direzione dei confini ucraini, è stato anticipato da una massiccia propaganda on line, veicolata attraverso i social media.
8. Szép-Wessel 2023.
9. Avverso la sentenza di primo grado, la ricorrente ha originariamente presentato un ricorso in Corte di giustizia, poi ritirato (causa C-620/22 P). La decisione del Tribunale è dunque divenuta definitiva a luglio 2023.

misure necessarie per rispondere alla grave minaccia alla pace alle frontiere dell'Unione e alla violazione del diritto internazionale possono includere un divieto temporaneo di radiodiffusione dei contenuti di alcuni media appartenenti, tra l'altro, ad un gruppo di canali, finanziato dal bilancio dello Stato russo, con la motivazione che essi sosterrebbero tale aggressione attraverso azioni di disinformazione orchestrata. Secondo la valutazione del Consiglio (v. i considerando dell'atto), queste azioni costituivano una minaccia consistente e diretta all'ordine pubblico e alla sicurezza dell'Unione, che giustificava il suo intervento nell'ambito delle competenze che il Trattato Ue gli riconosce. L'intervento del Consiglio è direttamente connesso alle finalità di salvaguardare i valori dell'Unione, i suoi interessi fondamentali, la sua sicurezza, la sua indipendenza e la sua integrità e, anche, a preservare la pace, a prevenire i conflitti e a rafforzare la sicurezza internazionale.

Da questo passaggio argomentativo emerge che il Tribunale dà rilievo particolare ad alcuni elementi: anzitutto il contesto di crisi internazionale e aggressione armata nel quale l'atto europeo si colloca, che rende la minaccia concreta per la sicurezza in Europa, come esplicitamente e correttamente evidenziato dal Consiglio nelle motivazioni dell'atto. Inoltre, la temporaneità del divieto di trasmissione di contenuti, che collega la misura alla minaccia. Infine, l'elemento oggettivo di collegamento tra il bilancio dello Stato aggressore e i canali di trasmissione dei contenuti.

All'interno di questo ben determinato perimetro, il Tribunale ritiene che "la propaganda e le campagne di disinformazione sono tali da mettere in discussione i fondamenti delle società democratiche e fanno parte integrante dell'arsenale di guerra moderna", ragione per cui le misure restrittive censurate si inseriscono anche negli obiettivi PESC e dunque il Consiglio ha la legittimazione ad adottare la decisione.

3.2. Il bilanciamento

Le misure restrittive si inseriscono «in un contesto straordinario e di estrema urgenza» e «fanno parte integrante di una serie di misure di portata inedita adottate dal Consiglio tra l'ultima settimana del mese di febbraio, durante la quale ha avuto luogo, il 21 febbraio 2022, la prima violazione dell'integrità territoriale dell'Ucraina, quando il presidente russo ha riconosciuto l'indipendenza e la sovranità delle regioni di Donetsk e di Lugansk e ha dato l'ordine alle sue forze armate di entrare in tali zone […]. Il rapido aggravamento della situazione e la gravità delle violazioni commesse hanno reso difficile qualsiasi forma di modulazione delle misure restrittive dirette a impedire l'estensione del conflitto. In tale contesto, l'Unione ha dunque reagito rapidamente, a fronte di una violazione di obblighi erga omnes imposti dal diritto internazionale, al fine di contrastare, con tutte le misure di cui disponeva che non comportavano l'uso della forza, l'aggressione militare dell'Ucraina da parte della Federazione russa» (par. 86).

Per preservare «l'integrità del dibattito democratico in seno alla società europea» era imperativa ed urgente la necessità di adottare misure restrittive di contrasto alle minacce ibride, incluse le misure nei confronti degli organi di informazione, controllati direttamente o indirettamente dalla leadership di un Paese aggressore, in quanto «fonte di un'attività continua e concertata di disinformazione e manipolazione dei fatti». Le «circostanze molto particolari del caso in questione», identificate nello «scoppio di una guerra alle frontiere dell'Unione», giustificano la massima rapidità nelle azioni per garantire l'effetto utile del contenimento della propaganda favorevole all'aggressione militare dell'Ucraina.

Circa la violazione della libertà di espressione e d'informazione garantita dall'articolo 11 della Carta dei diritti fondamentali dell'Ue, il Tribunale ribadisce che il rispetto dei diritti fondamentali si impone anche al settore PESC. La libertà di manifestazione del pensiero, peraltro, come tutte le libertà fondamentali può essere soggetta a limitazioni. Ad esempio, dalla giurisprudenza della Corte EDU emerge che la libertà di stampa su questioni di interesse generale è protetta a condizione che gli organi di stampa «agiscano in buona fede, sulla base di fatti esatti, e forniscano informazioni "affidabili e precise" in conformità con l'etica giornalistica o, in altri termini, nel rispetto dei principi di un giornalismo responsabile». Per contro, «le dichiarazioni che sostengono o giustificano la violenza, l'odio, la xenofobia o altre forme di intolleranza di solito non sono protette».

Per essere conformi al diritto dell'Unione, i limiti alla libertà di espressione devono rispettare le condizioni enunciate all'articolo 52, par. 1, della Carta, che corrispondono nella loro sostanza a quelle evidenziate dalla Corte EDU.

In primo luogo, la limitazione deve essere «prevista dalla legge», nel senso che l'istituzione dell'Unione che adotta misure in grado di restringere la libertà di espressione di una persona, fisica o giuridica, deve disporre di una base legale. La "riserva di legge" si intende rispettata se le restrizioni sono previste in atti di portata generale che presentano basi giuridiche chiare nel diritto dell'Unione. Nel caso di specie, tali basi sono rinvenute nell'articolo 29 TUE, per quanto riguarda la decisione impugnata, e nell'articolo 215 TFUE, per quanto riguarda il regolamento impugnato. Secondo il Tribunale, «tali disposizioni dei Trattati sono sufficientemente prevedibili per gli interessati» nei loro esiti.

Riguardo al divieto di intaccare il nucleo essenziale del diritto fondamentale – la seconda delle condizioni richieste –, rilevano sia il carattere temporaneo e reversibile delle misure restrittive (applicabili fino al 31 luglio 2022 e poi da riesaminare di volta in volta); sia la perimetrazione della temporanea sospensione di diffusione, che non impedisce alla ricorrente di diffondere contenuti al di fuori dell'Unione o di esercitare nell'Unione attività diverse dalla radiodiffusione, come la ricerca, le interviste e altre attività potenzialmente generatrici di redditi.

La terza condizione è soddisfatta ove sussista un obiettivo di interesse generale. Nel caso di specie, sussiste un obiettivo di interesse per la comunità internazionale: porre fine allo stato di guerra e alle violazioni del diritto internazionale umanitario, che la guerra può generare. In una prospettiva interna, le misure sono funzionali a tutelare l'ordine pubblico e la sicurezza dell'Unione, «minacciati dalla sistematica campagna internazionale di propaganda messa in atto dalla Federazione russa, tramite mezzi di comunicazione controllati direttamente o indirettamente dalla sua leadership, al fine di destabilizzare i paesi vicini, l'Unione nonché i suoi Stati membri e di sostenere l'aggressione militare dell'Ucraina». Tali scopi rientrano nella PESC e nella necessità «di salvaguardare i valori dell'Unione, i suoi interessi fondamentali, la sua sicurezza e la sua integrità». Le misure in particolare si inseriscono in un ampio quadro di sanzioni, che costituiscono una «risposta rapida, unificata, graduale e coordinata, attuata dall'Unione mediante l'adozione di una serie di misure restrittive, al fine ultimo di esercitare la massima pressione sulle autorità russe, affinché queste pongano fine alle iniziative e alle politiche che destabilizzano l'Ucraina nonché all'aggressione militare di tale paese». In questa prospettiva, dunque in ultima analisi, con gli atti impugnati si mira «a preservare la pace, prevenire i conflitti e rafforzare la sicurezza internazionale, conformemente agli obiettivi e ai principi della Carta delle Nazioni Unite». Le misure restrittive in questione possono essere intese anche come «la reazione, con i mezzi pacifici a disposizione dell'Unione e al fine di raggiungere gli obiettivi di cui all'articolo 3, paragrafo 5, TUE, di un soggetto di diritto internazionale a un atto di aggressione in violazione dell'articolo 2, paragrafo 4, della Carta delle Nazioni Unite e, di conseguenza, a una violazione degli obblighi erga omnes imposti dal diritto internazionale»[10].

La quarta condizione richiesta è la proporzionalità. Sul punto risultano rilevanti l'accertamento in atti del finanziamento del gruppo editoriale attraverso il bilancio dello Stato russo e l'assenza di elementi idonei a dimostrare indipendenza editoriale e autonomia istituzionale. Inoltre, è stato dimostrato mediante elementi di prova che la ricorrente avesse lanciato iniziative continue e concertate di propaganda prendendo di mira la società civile dell'Unione e dei paesi limitrofi, in particolare nell'intento di giustificare e sostenere l'aggressione nei confronti dell'Ucraina da parte della Federazione russa. Ciò emerge sia dal linguaggio utilizzato nelle trasmissioni, sia dalla narrazione delle operazioni militari come un'azione difensiva legittima della Federazione russa, di

10. Risoluzione del 2 marzo 2022, intitolata *Aggressione contro l'Ucraina* (A/ES-11/L.1), dell'Assemblea generale delle Nazioni Unite. In quest'ultima, considerando che la mancanza di unanimità tra i membri permanenti del Consiglio di sicurezza aveva impedito a quest'ultimo di adempiere al suo compito primario in materia di mantenimento della pace e della sicurezza internazionali, l'Assemblea generale delle Nazioni Unite ha deplorato l'aggressione dell'Ucraina commessa dalla Federazione russa in violazione dell'articolo 2, paragrafo 4, della Carta delle Nazioni Unite e chiesto che la Federazione russa cessi immediatamente l'uso della forza contro l'Ucraina e immediatamente ritiri completamente e incondizionatamente tutte le sue forze militari dal territorio dell'Ucraina entro i suoi confini riconosciuti a livello internazionale.

fronte alle minacce dei paesi occidentali, nonché alle provocazioni ucraine. Dagli elementi di prova si evidenzia una mancanza di equilibrio nell'informazione e dei principi relativi ai "doveri e responsabilità" degli organi di informazione audiovisivi.

Le limitazioni si dimostrano inoltre appropriate, cioè idonee a conseguire gli obiettivi di interesse generale perseguiti dall'Unione, che, in particolare, sono due: «proteggere l'ordine pubblico e la sicurezza dell'Unione e preservare l'integrità del dibattito democratico all'interno della società europea, la pace e la sicurezza internazionale»; e «esercitare la massima pressione sulle autorità russe, affinché pongano fine alle loro azioni e politiche che destabilizzano l'Ucraina nonché all'aggressione militare contro tale paese». Altre misure meno restrittive non avrebbero consentito di conseguire questi risultati. Ad es., il divieto di radiodiffusione in taluni paesi dell'Unione o un divieto limitato a talune modalità di radiodiffusione dei programmi o la limitazione a taluni tipi di contenuti, o ancora l'obbligo di apporre un banner o un'avvertenza, «non consentono di raggiungere altrettanto efficacemente gli scopi perseguiti dagli atti impugnati». Il Tribunale conclude così per la legittimità delle sanzioni adottate: gli obiettivi della pace e della sicurezza internazionale, cui le misure sono ricondotte, sono destinati a prevalere sulle conseguenze negative, anche notevoli, di tali misure per taluni operatori dell'informazione[11].

Il presente lavoro si inserisce nell'ambito del progetto "Innovazione e vulnerabilità: problemi giuridici e tutele" del Dipartimento di Giurisprudenza dell'Università di Macerata (finanziamento MUR, programma: Dipartimenti di Eccellenza 2023-2027) ed è parte del progetto Prin PNRR RightNets - Normative and Digital Solutions to Counter Threats during National Election Campaigns, finanziato dall'Unione europea - NextGenerationEU. I punti di vista e le opinioni espresse sono tuttavia solo quelli dell'Autrice e non riflettono necessariamente quelli dell'Unione europea o della Commissione europea. Né l'Unione europea né la Commissione europea possono essere ritenute responsabili per essi.

Riferimenti bibliografici

P. Moral (2022), *The Challenge of Disinformation for National Security,* in J. Cayón Peña (eds.), "Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts", Advanced Sciences and Technologies for Security Applications, Springer, 2022

S. Poli (2022), *La portata e i limiti delle misure restrittive dell'Unione europea nel conflitto tra Russia e Ucraina*, in SidiBlog.org, 22 marzo 2022

11. Questo scritto è stato chiuso senza poter esaminare una importante innovazione, di cui qui si dà solo menzione: il 12 dicembre 2023, la Commissione Ue ha presentato il *Defence of Democracy Package*, in vista delle elezioni europee 2024. Il pacchetto include una proposta di direttiva che stabilisce requisiti armonizzati nel mercato interno sulla trasparenza della rappresentanza di interessi esercitata per conto di paesi terzi. La proposta intende migliorare la trasparenza delle attività di rappresentanza di interessi per conto di paesi terzi finalizzate a influenzare lo spazio democratico. Del pacchetto fanno parte anche atti non vincolanti, che tuttavia saranno significativi per gli Stati membri competenti a gestire i processi elettorali: in particolare, una Raccomandazione sulla promozione del coinvolgimento e della partecipazione effettiva dei cittadini e delle organizzazioni della società civile ai processi di elaborazione delle politiche pubbliche e una Raccomandazione relativa a processi elettorali inclusivi e resilienti nell'Unione e al rafforzamento della natura europea e dell'efficienza nello svolgimento delle elezioni del Parlamento europeo. L'obiettivo di questo pacchetto è affrontare la minaccia delle ingerenze straniere, ritenute dalla maggioranza dei cittadini europei una priorità da considerare (*Eurobarometro*, 6 dicembre 2023). La raccomandazione sui processi elettorali mira a promuovere norme democratiche rigorose in materia di elezioni nell'Ue, promuove l'affluenza elettorale e una partecipazione inclusiva; affronta inoltre la questione della cyber-sicurezza delle infrastrutture connesse alle elezioni, proponendo misure volte a ridurre al minimo i rischi di ingerenza da parte di paesi terzi.

V. Szép, R.A. Wessel (2023), *Balancing restrictive measures and media freedom: RT France v. Council*, in "Common Market Law Review", vol. 60, 2023, n. 5

C.R. Sunstein (2017), *#Republic. La democrazia nell'epoca dei social media*, il Mulino, 2017

A. Tyushka (2022), *Weaponizing narrative: Russia contesting EUrope's liberal identity, power and hegemony*, in "Journal of Contemporary European Studies", vol. 30, 2022, n. 1

G.E. Vigevani, O. Pollicino, C. Melzi d'Eril, M. Cuniberti, M. Bassini (2019), *Diritto dell'informazione e dei media*, Giappichelli, 2019

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0129 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Arturo Di Corinto

Netwar, come cambia l'hacktivismo nella guerra cibernetica

La disponibilità delle tecnologie di comunicazione influenza le attività e la formazione stessa dei gruppi e dei movimenti della società civile. Con la diffusione di massa di Internet e del Web, la Rete è diventata un campo di battaglia per gli attivisti digitali. Molte delle pratiche di informazione, contestazione e sabotaggio tipiche dei movimenti di protesta sociale sono state digitalizzate e riversate in Rete. Protagonisti in questo scenario sono gli hacktivisti, gli hacker-attivisti che hanno usato la Rete per autorganizzarsi, fare propaganda, controinformazione, e condurre azioni politiche dirette. I loro obbiettivi e i loro metodi degli inizi erano quelli dell'infowar, la "guerra" d'informazione e propaganda, ma oggi gli hacktivisti sono entrati di prepotenza nelle guerre guerreggiate: spesso arruolati su una base ideologica, talvolta usati come mercenari, sono arrivati ad accompagnare i conflitti cinetici, le guerre vere e proprie. Si tratta di una mutazione graduale e forse attesa, ma poco presente nel dibattito pubblico e accademico. Con questo articolo vorremmo contribuire a tracciare l'evoluzione di questa trasformazione culminata nella creazione di vere e proprie milizie di hacktivisti digitali impegnati nel conflitto Russo-Ucraino.

Guerra dell'informazione – Guerra in Rete – Guerra cibernetica – Hacktivismo – Cybersicurezza

Netwar, hacktivism evolution in cyber warfare

The availability of communication technologies influences the activities and the very formation of civil society groups and movements. With the mass diffusion of the Internet and the Web, the Internet has become a battlefield for digital activists. Many of the infomration-related practices of information, protest and sabotage typical of social protest movements have been digitized and transferred online. The protagonists in this scenario are the hacktivists, who have used the Internet to self-organize, carry out propaganda activities, counter-information, and conduct direct political action. Their objectives and methods in the beginning were those of the infowar, the "war" of information and propaganda, but today the hacktivists have forcefully entered hybrid conflicts: often recruited on an ideological basis, sometimes used as mercenaries, have come to accompany kinetic conflicts, real wars. This is a gradual and perhaps expected mutation, but little present in the public and academic debate. With this article we would like to help trace of the evolution of this transformation which culminated in the creation of militias of digital hacktivists engaged in the Russian-Ukrainian conflict which is shaking Europe.

Infowar – Netwar – Cyberwar – Hacktivism – Cybersecurity

L'Autore è *Public Affairs and Communication Advisor* presso l'Agenzia per la cybersicurezza nazionale (ACN) e afferisce al Dipartimento di comunicazione e ricerca sociale di Sapienza - Università di Roma
Quanto dichiarato dall'Autore non impegna in alcun modo l'ACN

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Infowar, Netwar, cyberwar

Partiamo da una premessa, un conto è la contestazione digitale, l'infowar, altra cosa è la cyberwar che usa armi cibernetiche e viene praticata da eserciti, paramilitari e servizi segreti nel contesto dei conflitti tra Stati nazionali e mira a provocare danni a cose e persone. L'infowar è stata diversamente concettualizzata nella storia, ma ogni sua definizione operativa rimanda a una qualche forma di inquinamento dell'informazione.

Il defacciamento[1] dei siti (*web defacement*) di banche e governi, la creazione di luoghi digitali antagonisti in rete, i video virali del collettivo Anonymous, il cybersquatting[2] delle url e i siti clone di istituzioni come il Vaticano sono esempi di infowar, guerra dell'informazione[3]. E datano dalla metà degli anni Novanta del secolo scorso. Variamente concettualizati dai gruppi sociali, e da teorici come Ricardo Dominguez, Hakim Bey e Tommaso Tozzi[4], non implicano un danno irreversibile a cose e persone.

Nel novembre 1999, ad esempio, (r)TMark, gruppo di attivisti digitali, pubblica un sito[5] contente informazioni sul meeting di Seattle del 30 novembre del GATT (*Global Agreement on Tariffs and Trade*, predecessore del WTO, *World Trade Organization*). Il sito, formalmente identico a quello ufficiale dell'Organizzazione per il commercio mondiale, a dispetto alle aspettative dei visitatori mette in discussione gli assunti del libero mercato e della globalizzazione economica.

Nel febbraio 2001, invece, in occasione del Terzo Global Forum, quello sul governo elettronico tenutosi a Napoli il marzo successivo, alcuni attivisti napoletani clonano il sito della manifestazione ufficiale, ne modificano i contenuti e lo riversano su un loro dominio ocse.org che, successivamente censurato, viene trasferito sul sito www.noglobal.org/ocse. Anche in questo caso il sito plagiato dagli antiglobalizzatori conteneva una critica radicale al Forum che, secondo loro, era volto «a definire nuove modalità di sfruttamento e controllo sociale attraverso l'informatizzazione degli stati» anziché a promuoverne lo sviluppo democratico. In quell'occasione i contestatori digitali fecero anche un Netstrike (corteo telematico, antesignano dei

1. Con il termine *defacement* (in italiano *defacciamento*) si intende la modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.
2. *Cybersquatting*, o *domain squatting*, è l'attività di chi si appropria di nomi di dominio altrui corrispondenti a marchi commerciali, entità governative, personaggi famosi per realizzare un lucro sul trasferimento del dominio, per creare o un danno a chi non lo possa utilizzare oppure farne uno statement politico.
3. Di Corinto-Tozzi 2002; Di Corinto 2014.
4. Dominguez 2003; Bey 2007; Tozzi 2019.
5. https://web.archive.org/web/20120208220331/http://www.rtmark.com/gatt.html.

DDoS[6]), al sito di "FinecoOnLine"[7]) e lo usarono come occasione per avviare un dibattito pubblico sulla portata degli scambi finanziari on line e delle bolle speculative del mercato borsistico telematico.

Queste pratiche di attivismo digitale, o *hacktivism*[8], dall'unione delle due parole *hacking* e *activism*[9], non avevano niente a che vedere con le cyberguerre perché non miravano a distruggere e conquistare, ma ad occupare solo temporaneamente degli spazi di comunicazione per parlare all'opinione pubblica e ad una platea di altri cyberattivisti. Erano considerate pratiche di "guerriglia comunicativa" e di sabotaggio culturale[10].

L'antagonismo politico sociale in rete, secondo i suoi protagonisti, all'epoca rappresentava l'altra faccia della globalizzazione economica[11]. Così come si intensificavano gli scambi commerciali e l'economia diveniva "virtuale", così i movimenti sociali esprimevano bisogni universali "globalizzando la rivendicazione dei diritti" attraverso mezzi di comunicazione indifferenti alle frontiere e alle leggi degli Stati[12].

L'infowar degli hacktivisti (www.thehacktivist.com[13]) era qualcosa di assai diverso dalle cyberguerre e dal così detto "terrorismo informatico" o cyberterrorismo, e veniva praticata attraverso l'uso di *hacking skills* (capacità da hacker) per supportare l'azione diretta dei movimenti politici di base[14]. Gli hacker costruivano spazi e strumenti digitali per l'azione politica collettiva, come ad esempio strumenti di open publishing[15].

Il fax-strike, il Netstrike, il mass-mailing, il defacciamento dei siti web, sono le forme in cui in Italia, durante gli anni Novanta si è sovente articolata la protesta collettiva degli attivisti digitali. Seppure diversi, i *defacement* stessi – la sostituzione di una pagina web con un'altra o con un messaggio irridente e critico – somigliano da vicino alla copertura di un cartellone pubblicitario o alle scritte sui muri, sulla scia delle azioni degli attivisti del *Billboard Liberation Front*[16]. E anche in questo caso l'obiettivo era quello di appropriarsi di uno spazio per esprimere le proprie opinioni, anche quelle più estreme.

L'infowar è quindi per gli attivisti una guerra di parole, una guerra combattuta a colpi di propaganda, autorganizzata, dal basso. Ed è diversa dalla sua matrice linguistica che rimanda all'*Information Warfare*, intesa come un insieme di tattiche, tecniche e procedure belliche per assumere una superiorità informativa rispetto all'avversario tramite operazioni di spionaggio e sabotaggio[17].

2. La costruzione di uno spazio di *global public opinion*

Il concetto di infowar negli anni Novanta esonda dall'ambito militare e viene quindi appropriato dagli attivisti politici i quali, in aggiunta all'uso di strumenti tradizionali di comunicazione (volantini, affissioni, riviste), si "armano" di computer e cominciano ad usare la Rete come mezzo per comunicare le proprie ragioni ad una audience globale, sfruttando le peculiarità di un mezzo

6. DoS, *Denial of Service*, negazione di servizio ovvero blocco dei servizi web, causato da numerose richieste di accesso illegittime al servizio esposto. La sua variante più nota è il DDoS, il *Distributed Denial of Service attack*. Cfr. Brooks-Oxcelik-Oakley-Tusing 2021; Strano Network 1996
7. https://web.archive.org/web/20010201081900/http://www.netstrike.it/.
8. L'*hacktivism* è la convergenza dell'hacking con l'attivismo, dove "hacking" è qui usato per riferirsi a operazioni che sfruttano i computer in modi insoliti e spesso illegali, in genere con l'aiuto di software speciali ("strumenti di hacking"). In Denning 1999.
9. Denning 1999.
10. Critical Art Ensemble 1998; Piro 1998; Deseriis-Marano 2008.
11. .Zip!Puntozip 1997.
12. Klein 2000.
13. https://web.archive.org/web/*/www.thehacktivist.com.
14. Di Corinto-Tozzi 2002.
15. Veneziani 2006, pp. 210-220.
16. http://www.billboardliberation.com/.
17. Rapetto-Di Nunzio 2001.

potenzialmente accessibile a tutti da ogni dove, indipendentemente dalla collocazione spaziale e temporale degli attivisti e del pubblico per creare una nuova sfera pubblica[18]. Solo successivamente essi useranno la Rete come mezzo per realizzare azioni di interferenza sociale e di disobbedienza civile[19]. È in questo passaggio che i computer e la rete Internet diventano strumento e non solo teatro della contestazione, lo spazio dove la protesta, il rifiuto, la critica, espresse collettivamente, prendono forma e dalle parole si passa ai fatti. È questa la Netwar intesa come azione di guerriglia comunicativa e propaganda organizzata, che supera i concetti di blocco e sconfinamento in Rete tipici dell'infowar praticata dagli attivisti che così diventano Net Attivisti.

Ad esempio quando, nel 2014, in segno di protesta, gli attivisti digitali si coalizzano per impedire la sentenza capitale nei confronti del ventunenne Ali Mohammed al-Nimr, colpevole di aver incitato alla rivolta i suoi amici via SMS contro il governo saudita lanciando l'hashtag #OpNimr su Twitter, un elenco di tweet preimpostati che ogni net attivista può copiare, incollare e pubblicare, e solo dopo creando una lista di siti governativi da attaccare, riuscendo a mettere offline i siti del ministero dell'Economia e Finanze, della Giustizia e dell'Informazione del regime della famiglia Sahud con attacchi DDoS[20].

Infowar e Netwar sono quindi pratiche di conflitto tipiche dell'hacktivism, le cyberguerre no.

La cyberwar si riferisce alla guerra cibernetica propriamente detta, cioè a una guerra che usa l'informatica, la cibernetica e le reti di comunicazione al pari di armi convenzionali, per definizione appannaggio degli Stati e degli eserciti. La cyberwar, infatti, punta a smantellare i sistemi di comando, controllo e comunicazione del nemico in una maniera intenzionale e pianificata mettendo in campo ingenti risorse computazionali centralizzate facendo uso di cyber-armi come backdoor[21], botnet[22], malware[23], software exploits[24] e virus trojan[25], solo per citarne alcuni. La definizione generalmente accettata di guerra cibernetica, o cyberwar, è concettualizzata come una serie di attacchi informatici contro uno Stato-nazione, che causano danni significativi, dall'interruzione di sistemi informatici vitali fino alla perdita di vite umane. Secondo il *Tallinn Manual on the International Law Applicable to Cyber Operations* della Nato[26], un "attacco informatico" è «un'operazione informatica, offensiva o difensiva, che si prevede ragionevolmente possa causare lesioni o morte a persone o danni o distruzione di oggetti».

Questo tipo di guerra cibernetica, come tutte le guerre, produce tuttavia degli effetti di spillover anche sui civili, ad esempio interrompendo l'erogazione di energia elettrica all'interno di un

18. Meikle 2004.
19. Critical Art Ensemble 1998.
20. Di Corinto 2015.
21. Letteralmente "porta di servizio" collocata sul retro di un edificio. Viene chiamato così un canale occulto che consente l'accesso ad un sistema informatico eludendo le normali procedure di autenticazione.
22. Rete di computer utilizzata per attacchi da remoto, o per altre finalità, formata da computer infetti (*bot* o *zombie*) che, all'insaputa dei legittimi utenti, sono controllati da un utente malevolo (*botmaster*).
23. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo abusivo e nascosto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.
24. Software impiegato per lo sfruttamento di vulnerabilità di un sistema al fine di accedervi abusivamente o porre in essere azioni malevoli.
25. Tipologia di malware che cela le proprie funzionalità (ad es. accesso non autorizzato, furto di credenziali, sabotaggio del sistema target) all'interno di un software legittimo (il nome deriva dal mitico Cavallo di Troia). A tale attacco sono spesso associate tecniche di ingegneria sociale, che inducono il target a scaricare/installare il software contenente il trojan.
26. Schmitt 2017.

determinato territorio, come accadrà in Ucraina nel 2015 ad opera di gruppi paramilitari russi[27].

E tuttavia le tecniche usate nei conflitti telematici sono per definizione ibride e molteplici[28]. Così come la protesta digitale può determinare l'interruzione di un servizio – si pensi agli attacchi DDoS dimostrativi che bloccano temporaneamente la funzionalità di un sito web pubblico – la cyberwar può fare uso di tecniche di propaganda tipiche dell'infowar per accompagnare l'attacco vero e proprio[29].

Le tecniche di infowar usate dagli attivisti sono quindi inizialmente un miscuglio di campagne di informazione e di strategie comunicative derivate dall'arte di avanguardia che mirano a mettere in cortocircuito l'informazione istituzionale cannibalizzando l'attitudine al sensazionalismo tipico dei media mainstream – tv, radio e giornali –, prendendosi gioco delle veline d'agenzia di stampa e del modo di costruire la notizia[30]. Le campagne di informazione e controinformazione su Internet sono l'equivalente digitale di forme di comunicazione più tradizionali, tipiche dei movimenti politici di base, in cui l'e-mail sostituisce il volantino, la petizione elettronica sostituisce il banchetto di firme all'angolo della strada, il sito web i manifesti murali e i cartelloni. Finché, portando alle estreme conseguenze la logica del "panico mediatico", usato con successo dagli epigoni della Beat Generation[31], si producono notizie false per creare diffidenza e allarme. È il caso dei finti virus o della soffiata relativa ad una improbabile intrusione dentro sistemi informatici protetti che prelude alla Netwar.

La Netwar, la "guerra" nei network digitali, ma sarebbe meglio chiamarla "guerriglia", si presenta come una forma di azione diretta che punta a creare disturbo e interferenza, ma anche danni nelle attività di comunicazione dell'avversario, si tratti di una lobby politica o di una azienda multinazionale, un governo locale o sovranazionale[32]. Sono iniziative collettive e pubbliche di comunicazione radicale. È il caso dei DDoS[33], del synflood[34], dei virus artistici[35], della divulgazione di dati personali.

Le cyberguerre, al contrario, non mirano a delegittimare oppure a contrastare l'avversario attraverso la propaganda, piuttosto mirano a interrompere e sabotarne i flussi informativi, danneggiando le sue infrastrutture economiche e sociali.

Assaggi di queste cyberguerre si sono avute all'epoca della crisi fra Usa e Cina a causa della bomba recapitata "per sbaglio" all'ambasciata cinese di Belgrado durante la guerra del Kosovo (1998-1999). In quel caso i computer del Pentagono e della Nasa furono bersagliati da milioni di lettere elettroniche con virus (*mailbombing*). Oppure nel caso del conflitto telematico che vede combattersi fino ai giorni nostri israeliani e palestinesi. Già nel 2000 i giornali di Tel Aviv riportarono la notizia di un attacco informatico DDoS, che aveva messo fuori uso il sito ufficiale di Hezbollah, mentre cyber attivisti arabi avevano deturpato i siti dell'Università ebraica di Gerusalemme e dell'accademia di Netanya ed erano penetrati nel sito della difesa israeliano.

Da allora le forme e gli strumenti della cyberguerra condotta in maniera coperta dagli Stati attraverso i loro "proxy", siano essi paramilitari, servizi segreti o Stati canaglia, ha visto una costante evoluzione. Dall'uso del virus Stuxnet[36], di fabbricazione americana-israeliana, che nel 2010 ha bloccato le centrali per l'arricchimento dell'uranio a Natanz, Iran, fino all'uso del malware Black

27. Greenberg 2019.
28. Rapetto-Di Nunzio 2001; Curioni-Giannuli 2019.
29. Microsoft Digital Security Unit 2022.
30. Deseriis-Marano 2008.
31. Autonome A.f.r.i.k.a. gruppe-Blisset-Brunzels 2001.
32. Di Corinto 2001.
33. Deseriis 2017, pp. 131-152.
34. Il *Synflood* è un'interferenza nei protocolli di comunicazione per causare "l'inondazione" ovvero la saturazione di un servizio digitale; Critical Art Ensemble 1998.
35. Tozzi 2019.
36. Zetter 2015.

Energy creato dal gruppo russo Sandworm[37], che ha interrotto l'erogazione di energia elettrica in Ucraina nel 2015 lasciando al buio e al freddo 225 mila ucraini all'antivigilia di Natale[38].

3. L'Hacktivism, origini ed evoluzione

Prima c'era l'*activism*. L'azione politica diretta nello spazio fisico cittadino che si concretizzava negli scioperi, nei cortei, e nell'occupazione di strade (*Reclaim the streets*), piazze e edifici. Poi è venuto l'*hack-tivism*, l'azione diretta in Rete con tecniche di hacking, e i cortei e le occupazioni sono diventate virtuali, dal *Netstrike* ai *Distributed Denial of Services* (DDoS).

Il termine *hacktivism* deriva dall'unione delle parole *hacking* e *activism*[39]. L'*Hacking* è la messa in opera di una particolare attitudine verso le macchine informatiche che presuppone storicamente la pratica di studiare i computer per migliorarne il funzionamento attraverso la cooperazione e il libero scambio di informazioni tra i programmatori, e la condivisione del sapere risultante per dare a tutti accesso illimitato alla conoscenza in essi incorporata[40]. *Activism* è il termine americano che indica le forme dell'azione diretta praticate dai movimenti politici di base (*grassroots movements*) come i sit-in, i cortei, i picchetti.

Successivamente è stato concettualizzato il mediattivismo o *media activism*[41], che si è sostanziato nel racconto mediatico delle proteste di piazza e nella diffusione virale dell'informazione in Rete usando anche le immagini in movimento e le street tv. Infine, col Web 2.0 ha fatto la sua comparsa il *clicktivism*, l'adesione a petizioni, mobilitazioni e proteste, reali e virtuali, con un colpo di click, senza staccare gli occhi dallo schermo del computer. Ma mentre questa nuova modalità di partecipazione coinvolgeva i grandi numeri dei social network, a compensare questa ondata di "slacktivism" – termine gergale per indicate "l'attivismo fannullone", cioè quello che dopo il click si disinteressa della reale entità del cambiamento prodotto –, si è assistito al revival dell'*hacktivism* col defacciamento dei siti web, i virus politici, gli attacchi DDoS organizzati.

Cosa è accaduto? È accaduto che la rivoluzione digitale ha messo nelle mani di molti individui strumenti di comunicazione efficienti e a basso costo in grado di connettersi alla Rete, mentre le crisi economiche e finanziarie ripetute hanno risvegliato la coscienza delle ingiustizie e portato singoli, gruppi e movimenti digitali a riorganizzarsi su due fronti: la comunicazione e il sabotaggio.

I movimenti sociali in Rete hanno sempre avuto una grande quantità di iniziative legate alla comunicazione e il loro rapporto avanguardistico e sperimentale con gli strumenti della comunicazione ha prodotto le fanzine ciclostilate, le radio indipendenti, il videoteatro, il documentario politico, fino ai siti web e ai software di comunicazione gratuiti[42]. Dall'italiana Radio Alice a Seattle 1999, fino alle azioni di Anonymous, è possibile ripercorrerne il filo conduttore che passa per Indymedia, Wikileaks e il movimento Occupy Wall Street.

Gli ingredienti della messa in opera della contestazione sono uguali e diversi, rappresentano in molti casi l'evoluzione tecnica e la convergenza di strumenti e forme di comunicazione precedenti: personal media prima (dal fax ai telefoni cellulari, dai camcorder ai videotelefoni, dai siti ai blog); software gratuiti e open source per l'editing di testi, audio e video; l'ubiquità dell'accesso a Internet (dai *Bulletin Board Systems*, BBS, al wi-fi), e poi social network e piattaforme di blogging e whistleblowing. Una "rimediazione" che consente di riunire i singoli media, prima isolati, sulla stessa piattaforma (convergenza digitale), e di portare uno stesso contenuto su piattaforme o media differenti (la divergenza digitale)[43], per realizzare una produzione di informazione indipendente, dal basso, orientata al sabotaggio dei flussi di comunicazione

37. Greenberg 2019.
38. Cyber Infrastructure & Security Agency 2021.
39. Di Corinto-Tozzi 2002.
40. Levy 1996.
41. Pasquinelli 2002.
42. Downing-Villareal Ford-Gil-Stein 2001; Meikle 2004.
43. Bolter-Grusin 2000.

di un potere «che non risiede più in strutture stabili e definite»[44] ma è organizzato intorno a dati, messaggi e informazioni.

Se la creazione di tool come software, server e servizi di messaggistica per la comunicazione indipendente ha subito un arresto con l'affermarsi dei social network e del Web 2.0 – che ha portato anche i gruppi di attivisti più radicali ad avere un account Facebook (il Partito Pirata[45]) –, si sono sviluppate nuove forme di comunicazione e sabotaggio a cavallo tra l'estrazione di informazione protetta e la sua comunicazione al pubblico più ampio, con una strategia di *hack and leak* ovvero "hackera e diffondi"[46].

È il caso di Wikileaks: ottenere informazioni sensibili e offrire al pubblico quelle di cui il potere si vergogna è stata la sua arma più potente fin dalle origini[47], ma prima c'erano stati gli hacker del Chaos Computer Club[48] che negli anni Ottanta, penetrati nel sistema informatico del Comune di Berlino, avevano acquisito le informazioni sulle case comunali sfitte per passarle al movimento dei senza casa. E hanno fatto scuola. Anche l'hacking può ricorrere alla violazione di sistemi informatici protetti (cracking) se ha un fine etico.

Nell'attacco al sito della Corte costituzionale ungherese da parte di Anonymous[49] nel marzo 2012, gli hacktivisti col volto di Guy Fawkes hanno cambiato il testo della Costituzione autoritaria voluta dal presidente Viktor Orban affermando il "diritto alla ribellione", con queste parole: «Gli ideologi e i governanti della tirannia, o anche i dittatori, non rappresentano che brevi periodi della storia. Il popolo ha il diritto di eliminare la tirannia e ribellarsi», aggiungendo poi un comma specifico: «[chiediamo] la pensione a 32 anni per gli informatici con il 150 per cento dello stipendio»[50].

Il retroterra teorico di molti di questi guerriglieri dell'informazione è l'etica hacker delle origini: consentire a chiunque l'accesso all'informazione, dovunque essa sia riposta e comunque sia custodita, con la ferma convinzione che l'accesso all'informazione renda tutti più liberi di fare e di scegliere[51]. Il paradigma dell'azione è la condivisione di saperi e conoscenze e la difesa dei beni comuni che si producono nei circuiti dell'interazione sociale, e che, secondo gli attivisti, necessita di pratiche non ortodosse. È questa l'idea che afferma definitivamente quella pratica creativa e disordinata che definiamo di hacktivism, e che vedrà la galassia dei collettivi hacktivisti di Anonymous protagonisti per oltre un decennio.

Sono infatti hacktivisti gli Anonymous organizzatori dell'operazione Payback[52], condotta nel 2010 contro i grandi produttori di contenuti creativi, le major hollywoodiane e le loro rappresentanze di categoria, contro le autorità di garanzia quali l'Agcom italiana e le collecting societies come la Siae. In queste iniziative c'era tutta la virulenza della contestazione verso chi si appropria del sapere altrui mettendoci sopra un marchio e pretendendo di limitarne la diffusione e la conoscenza se non dietro al pagamento di ogni file tracciabile e certificato.

Questi soggetti del conflitto in Rete non sono solo precari dell'industria culturale sfruttati e depressi dalla mancanza di lavoro[53]. Molti sono lavoratori che, in puro stile hacker, di giorno lavorano a far funzionare la macchina burocratica degli Stati, mantengono le linee di comunicazione a cavallo degli oceani e scelgono il payoff di prodotti pubblicitari, mentre la notte disfano la loro tela di Penelope. Una moltitudine che non è fatta soltanto di una minoranza colta, istruita, con eccellenti competenze informatiche, perché gli attacchi

44. Critical Art Ensemble 1995.
45. https://it.wikipedia.org/wiki/Partito_Pirata.
46. Rid 2022.
47. Assange 2012.
48. https://www.ccc.de/en/.
49. Coleman 2016.
50. La Repubblica 2012.
51. Levy 1996; Di Corinto-Tozzi 2002.
52. Olson 2012.
53. Tiddi 2002; Berardi Bifo 2011.

più virulenti sono stati portati con strumenti facili da usare come il Loic, *Low Orbit Ion Cannon*[54], e scaricabili sotto forma di codici software da installare sul computer, usare e cancellare subito dopo, ottenendo di avvicinare alla protesta ogni tipo di insoddisfazione verso i poteri costituiti.

Organizzazione senza capi, ma con dei leader, sostituibili, che hanno portato il conflitto all'interno delle reti di CIA, governi e servizi segreti, dal 2004 ad oggi Anonymous si presenterà come il capostipite di una nuova generazione di hacktivisti che conduce battaglie sociali a colpi di mouse e che agiscono per contagio ed emulazione[55].

In tutto questo, l'emergere di una nuova socialità è stato modellato dalla Rete assumendo molte forme. Dagli Indignados spagnoli a quelli greci, che però hanno costruito i loro propri social network al riparo dei dipartimenti di intelligence di tutto il mondo i quali usano Facebook e X (Twitter) per controllare i movimenti sociali, difendendosi dall'espropriazione dei propri dati per finalità commerciali. Tra queste si annoverano quelle scelte dai giovani magrebini che durante la così detta Primavera Araba tra il 2010 e il 2011 attraverso Facebook e YouTube hanno trovato le parole per contestare le dittature, si sono uniti ai coetanei per non sentirsi più soli e trovare il coraggio di scendere in piazza, anche a costo di farsi ammazzare, come quando nella Casbah di Tunisi nel 2010 furono «allestite tende e gruppi di lavoro che si occupavano di Internet, media e attivismo in rete»[56].

Così il sapere comunicativo diffuso dei "Millennial", unito alla potenzialità della comunicazione telematica ha prodotto i nuovi contestatori della rete in un procedimento alchemico accelerato dalla crisi globale, che è crisi della finanza, dell'economia, della società, della rappresentanza democratica, dello Stato-nazione[57].

Dietro alle loro sortite c'era una consapevolezza, teorizzata da Hakim Bey[58], e Ricardo Dominguez del Teatro del disturbo elettronico[59], per la quale il potere, da materiale che era, si stava sempre più smaterializzando e non coincideva più con luoghi fisici, portaerei e palazzi, ma coi flussi di comunicazione digitale che possono essere dirottati o sabotati.

Gli hacktivisti oggi però non sono più i soggetti del conflitto sociale in rete che rivendicavano dignità e libertà, reddito e tempo libero, democrazia e giustizia, autodeterminazione.

4. La nuova era dell'hacktivism, l'occupazione dell'agenda mediatica e dei flussi di comunicazione

L'hacktivism è stato a lungo associato a gruppi come Anonymous, gruppi decentralizzati e destrutturati composti da privati cittadini con differenti background. Anonymous ha lanciato numerose campagne (chiamate "Operazioni" e introdotte dal prefisso #Op) contro target individuati in base alle inclinazioni e agli interessi dei suoi membri. Tra le più note, l'operazione contro la chiesa di Scientology, che segna l'avvio del fenomeno, e l'operazione PayBack contro la Sony Corporation. Come racconta Geoff White[60], gli hacktivisti hanno spesso incarnato, in varia misura, una cultura tecnocratica, creativa, e ludica, ma chiunque, a prescindere dalla fede politica, è sempre stato il benvenuto nei gruppi di hacktivisti che si rifacevano alla galassia di questi "anonimi" nati sul forum visuale 4Chan e che avevano un solo imperativo, "Non attaccare i Media".

Altre iniziative di questi hacktivisti old school includono campagne come l'Operazione KKK di Anonymous contro i membri e sostenitori del Ku Klux Klan[61], l'Operazione Lolita, il cui obiettivo era quello di fermare lo smercio di pedopornografia in Rete, fino ad arrivare alle azioni della corrente scissionista di Anonymous, LulzSec, responsabile di attacchi informatici eclatanti alla HBGary, società

54. Di Corinto 2010.
55. Goode 2015, pp. 74-86.
56. Massarelli 2012, p. 40.
57. Klein, 2000.
58. Bey 2007.
59. Dominguez 2003.
60. White 2022.
61. Di Corinto 2014.

di cybersicurezza che aveva lavorato a incastrare sia gli Anonymous sia Julian Assange, il fondatore di Wikileaks, e che, da loro hackerata, ha dovuto terminare le attività.

Altre campagne, di profilo opposto tra di loro, a dimostrazione della variabilità di interessi dei gruppi eterogenei di hacktivisti che di volta in volta usano la sigla Anonymous per le proprie rivendicazioni, sono state #OpIsrael e #OpPalestine e, nel 2016, #OpTrump e #OpHilaryClinton.

Dal 2020 ad oggi però l'hacktivism ha cambiato natura. Per effetto di numerosi conflitti, locali e regionali, in uno scenario geopolitico dalle frontiere mobili, alcuni gruppi hacker hanno modificato le loro attività e la loro attenzione rispetto all'ideologia dell'azione diretta che mira al cambiamento sociale. Il fenomeno dell'hacktivism oggi non sembra più riguardare gruppi eterogenei, le crew, che si uniscono temporaneamente intorno a parole d'ordine precise, o a una causa specifica, il *single issue activism*, per vendicare un comportamento o riparare un torto. Oggi i gruppi di hacktivisti sono strutturati e organizzati con strumenti di attacco/difesa sofisticati e vengono supportati dai governi seppure raramente in maniera esplicita, fatta eccezione per l'IT Army ucraino[62] quando i primi cyberattacchi che hanno accompagnato l'invasione russa dell'Ucraina nel 2021 hanno generato la chiamata alle armi dei cittadini ucraini, e migliaia di attivisti hanno bloccato per ore banche e ministeri russi e, presumibilmente aiutati dai servizi di intelligence occidentali, rubato dati governativi usando il nome di Anonymous come copertura.

Le imprese, i governi e le infrastrutture critiche di molti paesi sono stati bersagliati da questa forma di hacktivism. Dal 2021 al 2023 tutti i paesi del G20 hanno subito pesanti attacchi mossi dai gruppi di attivisti, che in alcuni casi hanno avuto un impatto significativo. Gli attacchi recenti, per lo più di tipo DDoS, hanno interessato non solo i governi di questi paesi, ma anche grandi aziende come Lockheed Martin, azienda americana operante nel campo della difesa.

In questo contesto, il conflitto Russo-Ucraino, successivo all'invasione russa del Donbass, ha rappresentato un forte elemento di stimolo alla partecipazione degli hacktivisti nelle azioni collaterali alla guerra che ne è divampata.

5. Il caso di studio di Killnet, Legion e NoName(057)16

I principali gruppi di hacktivisti che hanno agito negli ultimi due anni condividono diverse caratteristiche proprie delle organizzazioni strutturate: una chiara ideologia politica, una gerarchia dei membri e una leadership definita, con un processo di reclutamento formale. Gli specialisti dell'IT Army Ucraino, ad esempio, in una prima fase sono stati selezionati attraverso l'analisi dei curricula e a monte di un continuo processo di reclutamento sui canali Telegram[63]. Sul fronte opposto, quello russo, è stato messo a disposizione degli hacktivisti un sofisticato tool di attacco come parte del DDoSia project realizzato dagli hacktivisti filorussi di NoName(057)16[64].

Lanciato nel 2022 e successore della botnet Bobik, lo strumento di attacco DDoSia è progettato per mettere in scena attacchi DDoS contro obiettivi situati principalmente in Europa, Australia, Canada e Giappone. Nel periodo che va dall'8 maggio al 26 giugno 2023 i paesi più attaccati sono stati Lituania, Ucraina, Polonia, Italia, Repubblica Ceca, Danimarca, Lettonia, Francia, Regno Unito e Svizzera per un totale di 486 diversi siti web colpiti. Le implementazioni di DDoSia basate su Python e Go scoperte fino ad oggi lo rendono un programma multipiattaforma in grado di essere utilizzato su sistemi Windows, Linux e macOS. DDoSia viene distribuito attraverso un processo completamente automatizzato su Telegram che consente alle persone di registrarsi all'iniziativa di crowdsourcing in cambio di un pagamento in criptovaluta e di un archivio .zip contenente il toolkit di attacco. Ciò che è degno di nota della nuova versione è l'uso della crittografia per mascherare l'elenco degli obiettivi da attaccare, un fatto che dimostra come lo strumento venga mantenuto attivamente dagli operatori.

I gruppi hacktivisti si coordinano quindi nella selezione dei bersagli, si coalizzano, si fondono, e collaborano, svolgendo anche consistenti attività di propaganda finalizzate a pubblicizzare

62. https://t.me/itarmyofukraine2022.
63. https://t.me/itarmyofukraine2022/1637.
64. https://t.me/c/1228309110/34219.

e promuovere i loro risultati, veri o presunti che siano, sui canali Telegram, sul Web e in televisione, come accaduto per Killnet, di cui parleremo più avanti. Questi hacktivisti, secondo i rapporti di Microsoft e Google/Mandiant[65], si mobilitano in seguito a eventi politici, e operano di concerto con enti governativi, raggiungendo obiettivi strategici e ad ampio spettro con un discreto tasso di successo, e un maggiore impatto sociale favorito dal sensazionalismo mediatico di questi attacchi.

L'evoluzione di questa forma di hacktivism è iniziata, secondo alcune ricerche, silenziosamente, nel Medio Oriente ad opera di diversi gruppi come Hackers of Savior, Black Shadow e Moses Staff. Tali gruppi hanno concentrato gli attacchi esclusivamente su Israele. La maggior parte di questi non ha nascosto i rapporti con la propaganda antisraeliana promossa dal regime iraniano. Parallelamente, altri gruppi, fra i quali Predatory Sparrow, si sono concentrati nell'attacco di bersagli iraniani e pro-iraniani: il loro unico piano comune essendo l'opposizione al regime degli Ayatollah.

In realtà l'embrione di queste attività, basate su individuazione del nemico con strumenti di Open Source Intelligence (Osint)[66], tramite l'esfiltrazione di dati strategici, la corruzione dei database avversari, fino all'inoculazione di malware, va rintracciato nel mondo hacktivista nella guerra senza quartiere che Anonymous – chiunque si celasse sotto questa sigla – ha condotto contro l'Isis[67].

L'hacktivism adesso è parte essenziale della guerra ibrida combattuta tra la Federazione Russa e l'Ucraina. Mentre una serie di attacchi, contro l'Estonia nel 2007, la Georgia nel 2008, l'Ucraina nel 2014, hanno ricevuto una provvisoria attribuzione – si tratterebbe infatti di paramilitari e servizi segreti russi, in particolare del GRU, il servizio segreto militare russo e solo in misura ridotta di hacktivisti –, nella prima parte del 2021, sono emerse altre formazioni, evidenziando un rapporto più diretto tra criminalità cibernetica, hacktivism e hacking di Stato.

Secondo Google-Mandiant[68], quando gli hacker governativi russi attaccano, passano i dati rubati agli hacktivisti entro 24 ore dall'irruzione in modo da consentire loro di effettuare nuovi attacchi e diffondere propaganda filorussa. Ad agire in questo modo sarebbero in particolare quattro gruppi non governativi: XakNat Team, Infoccentr, CyberArmyofRussia_Reborn e Killnet.

Tuttavia, mentre XakNat si coordinerebbe con l'intelligence russa, Killnet, con cui collabora, è pronta ad attaccare chiunque se pagata. Nel corso del 2022 il collettivo, che ha anche bersagliato l'Italia, ha però incominciato ad ammantare le proprie azioni di patriottismo, diventando una celebrità grazie alle ospitate nella televisione russa.

Negli gli ultimi mesi del 2022 e per tutto il 2023, NoName057(16) ha individuato come obiettivi degli attacchi i Paesi nell'Unione Europea dichiaratamente impegnati a sostenere l'Ucraina come Polonia, Lituania, Lettonia, Slovacchia e Finlandia, nonché l'Italia, a più riprese. NoName057(16) ha anche attaccato il sito del parlamento finlandese, dopo che la Finlandia aveva espresso interesse nell'unirsi alla NATO.

Il gruppo ha apertamente dichiarato i propri piani a supporto degli interessi russi, come emerge nel manifesto di NoName057(16)[69], che ha indirizzato, con regolarità, gli attacchi verso l'Ucraina con l'intenzione di espandere il proprio raggio d'azione.

L'altro schieramento è composto da altrettanto numerosi gruppi di hacktivisti che si sono mobilitati per sostenere l'Ucraina. Alcuni, come l'Esercito IT ucraino, sono ufficialmente controllati dal governo. L'IT Army è stato creato qualche giorno dopo l'inizio dell'invasione russa e comprende volontari provenienti da tutto il mondo per sostenere l'Ucraina seguendone le direttive, ma è composto anche da esperti dell'intelligence ucraina. Ad affiancarli in alcune azioni eclatanti il gruppo Ghostsec, noto almeno dal 2015 per le incursioni contro il cybercaliffato, la cyber-unit dell'Isis, quando, staccatisi da Anonymous, hanno incominciato a occuparsi di cyber-intelligence e antiterrorismo

65. Mandiant Intelligence 2022.
66. Osint è la raccolta di informazioni da fonti aperte
67. Di Corinto 2015a.
68. Mandiant Intelligence 2022.
69. Ninotti-Colatin 2022.

per trasformarsi poi in GhostSecSecurity prima di scomparire e riapparire nel cyberspace del conflitto russo-ucraino con lo stesso nome[70].

Secondo l'azienda di sicurezza informatica CyberKnow a maggio 2023 si contavano 112 gruppi di hacker attivisti che parteggiano per l'una o per l'altra parte nel conflitto russo ucraino (figura 1).

Figura 1. A maggio *2023 sono 112 i gruppi hacktivisti attivi nel conflitto russo-ucraino copyright CyberKnow*

Uno dei maggiori attori hacktivisti all'interno di questa galassia resta Killnet, un gruppo che è stato pubblicamente annunciato attorno al febbraio 2022, all'inizio del conflitto russo-ucraino. Durante la guerra in Ucraina ha rivendicato attacchi DDoS ai siti governativi rumeni, polacchi e di aziende americane. Sul proprio canale Telegram ha dichiarato che il suo obiettivo è attaccare "i Paesi Nato e l'Ucraina".

Il collettivo Legion ad essi affiliato si presenta come una versione russa di Anonymous. Perlomeno ne emulano il linguaggio e l'estetica sia nei messaggi che nelle immagini. Ma a differenza di Anonymous, che dopo l'invasione russa si è apertamente schierato a favore dell'Ucraina, Legion sostiene azioni a favore della Russia. Killnet è diventato piuttosto noto dopo il 3 aprile 2022, da quando cioè un altro gruppo di hacker, Bluehornet/Atw, ha diffuso alcuni dati personali di quelli che sarebbero alcuni dei leader del gruppo e rivelato l'esistenza della botnet di Killnet. Bluhornet è un gruppo antagonista di Killnet nella controparte virtuale della guerra cinetica tra Russia e Ucraina.

Il gruppo ha iniziato le sue attività aggressive a marzo 2022, con obiettivi primariamente ucraini, ma già ad aprile il gruppo aveva completamente cambiato l'oggetto della sua attenzione supportando gli interessi geopolitici russi in tutto il mondo. Tra fine febbraio e settembre 2022, il gruppo ha affermato di aver portato a termine più di 550 attacchi. Solo 45 di questi però erano indirizzati all'Ucraina: meno del 10% del numero di attacchi totale[71].

Molti di questi attacchi erano diretti a obiettivi di alto profilo come i principali siti governativi, grosse compagnie finanziarie, aeroporti e altri bersagli. Mentre in alcuni casi è difficile comprendere l'impatto reale, in altri casi gli attacchi hanno chiaramente avuto successo, provocando l'inattività

70. Di Corinto 2022.

71. Check Point Research 2022.

dei principali siti web, molti dei quali fornitori di servizi pubblici essenziali.

Ecco di seguito alcuni esempi.

1. A marzo, l'aeroporto internazionale di Bradley in Connecticut (US) ha subìto un attacco DDoS che ha interessato il proprio sito web. Le autorità statunitensi hanno confermato un tentato attacco DDoS su larga scala sul sito dell'aeroporto.

2. Ad aprile, alcuni siti web che appartengono al governo rumeno, come quello del Ministero della Difesa, quello della Polizia di Confine, quello della Compagnia Nazionale dei Trasporti Ferroviari e una banca commerciale, sono stati resi irraggiungibili per diverse ore. Questi attacchi si sono verificati in risposta ad una affermazione fatta dal leader rumeno del partito Socialdemocratico Marcel Ciolacu, che si è offerto di procurare armi all'Ucraina.

3. A maggio, ingenti attacchi DDoS sono stati portati a termine contro due fra i maggiori Paesi europei:

– sono stati coinvolti diversi bersagli tedeschi, incluso il governo e siti web dei politici, fra questi, il sito del partito a cui appartiene il cancelliere Olaf Scholz, il sito del Ministero della Difesa, quello del Parlamento, quello della Polizia Federale e diverse autorità della polizia statale. Secondo gli osservatori, una risposta agli sforzi dell'amministrazione Scholz di fornire equipaggiamento militare all'Ucraina, autorizzando il trasferimento di 50 Gepard anti-aircraft, e annunciando la consegna di 7 sistemi di artiglieria semoventi e a fuoco rapido.
– Anche il Senato italiano, il Ministero della Difesa e l'Istituto superiore di sanità sono stati presi di mira con attacchi da negazione di servizio ai propri siti web.

4. A giugno, due significative onde di attacchi sono state portate a termine contro la Lituania e la Norvegia in risposta agli sviluppi geopolitici che sono avvenuti fra questi Paesi e la Russia:

– seguendo la decisione del governo lituano di fermare il transito di beni russi verso Kaliningrad, un'ondata rilevante di attacchi ha colpito i servizi pubblici lituani e il settore privato. Durante l'attacco, Jonas Skardinskas, il capo della cybersecurity presso il Centro di Cyber Sicurezza Nazionale Lituano, ha avvisato che i disagi con i trasporti, i settori finanziari e quello energetico sarebbero potuti continuare per diversi giorni amplificando l'impatto dell'attacco. Ad un certo punto la maggioranza dei siti web lituani non era accessibili tramite indirizzi IP esterni al paese, più probabilmente come misura preventiva finalizzata a mitigare la portata dell'attacco.
– Lo stesso mese, diverse organizzazioni norvegesi sono state disconnesse. Si pensa che questo attacco sia stato eseguito come risultato di una disputa riguardante il transito attraverso il territorio norvegese verso un estrattore di carbone sotto il controllo russo situato nell'Artico.

5. A luglio, Killnet ha concentrato i propri sforzi sulla Polonia e causato l'indisponibilità di molti siti web. Molti degli attacchi sono stati diretti ai portali governativi, le autorità di tassazione e i siti web della polizia.

6. Agosto è stato un mese piuttosto intenso per Killnet. È cominciato con un attacco in Lettonia: dopo aver dichiarato la Russia come "un Paese rappresentante del terrorismo", il sito del Parlamento ha subìto un ingente attacco DDoS. Successivamente (nello stesso mese), l'Estonia ha affrontato l'attacco più esteso da quello del 2007, effettuato in risposta alla rimozione del monumento al soldato sovietico. L'efficacia di questi attacchi è stata discutibile, in quanto sembra che l'Estonia fosse ben preparata per questo genere di eventualità. Ad agosto, Killnet ha anche iniziato a concentrarsi sugli USA. Il gigante della produzione americana Lockheed Martin è stato pesantemente bersagliato da Killnet come conseguenza del rifornimento al sistema militare dell'esercito ucraino. Parallelamente Killnet ha anche bersagliato la US Electronic Health Monitoring e Tracking System e il Senato statunitense, che stava dibattendo la possibilità di inviare un aiuto addizionale all'Ucraina.

7. A settembre il gruppo ha bersagliato l'Asia per la prima volta indirizzando i suoi sforzi in particolare al Giappone, a causa del supporto giapponese all'Ucraina.

6. Disinformazione ed interferenze hacker

Con l'evolversi del conflitto scaturito dalla contesa delle Isole Kuril, Killnet ha attaccato con successo diversi siti giapponesi, incluso l'e-government, i siti

di trasporto pubblico della città di Tokyo e Osaka, i sistemi di pagamento JCB e Mixi, il secondo più grande sito web giapponese.

Come ci sono riusciti? I più grandi gruppi di hacktivisti che sono emersi nel corso degli ultimi due anni sono caratterizzati da operazioni ben strutturate che li mettono nelle condizioni di essere efficaci e di attrarre persone con maggiori skill. Queste persone sono solitamente motivate da una chiara ideologia legata allo Stato e i loro obiettivi sono parte di un manifesto che contiene un elenco di regole da seguire.

Per esempio, Killnet ha più di 100.000 iscritti nei suoi canali Telegram ed «è organizzata secondo una struttura militare con una gerarchia marcatamente top-down. Killnet consiste in un insieme di squadre preparate ad eseguire attacchi che rispondono ad un ordine principale. Attualmente esistono una dozzina di sottogruppi fra i quali il primario è Legion. Tutti questi gruppi sono guidati da un hacker anonimo con nickname KillMilk, che ha annunciato la sua intenzione di distaccarsi dal gruppo a luglio, rimanendo ancora coinvolto nelle attività del gruppo. Legion e le squadre (conosciute come: "Jacky", "Mirai", "Impulse", "Sakurajima", "Rayd", "Zarya", "Vera", "Phoenix", "Kajluk", "Sparta" and "DDOSGUNG") sono considerate le forze speciali di Killnet, con Legion identificata come la sua forza di cyber-intelligence»[72].

Tanti piccoli team organizzati attorno al maggiore gruppo e al suo leader, che assegna ordini d'attacco a ciascun capogruppo dando vita a infrastrutture indipendenti e migliorando così le probabilità di sopravvivenza dell'intera organizzazione. Questo metodo si è dimostrato efficace dal momento che la squadra continua a reclutare membri, crescendo numericamente. La pagina Telegram contiene regole, discussioni riguardanti gli obiettivi e le istruzioni rispetto a creare/unirsi a nuove squadre per i membri che cercano autonomia o un avanzamento gerarchico. L'evoluzione di Killnet li ha messi nella situazione in cui gli altri gruppi vogliono collaborare con loro, o ufficialmente unire le forze.

Un nuovo interessante fenomeno riguarda i metodi di reclutamento del gruppo. Diversamente da Anonymous, che è orgoglioso di dare il benvenuto a chiunque, senza imporre alcun prerequisito riguardante skill o piani specifici, la nuova era hacktivista accetta solo membri che rispettano prerequisiti minimi. Molti gruppi, come Killnet e le sue squadre, scelgono di investire in programmi di recruitment, pubblicizzati sui propri canali Telegram. Alcuni gruppi hanno istituito un processo di preselezione per assumere solo hacker competenti o esperti di un particolare campo, per ridurre il rischio di fare errori che potrebbero compromettere le operazioni.

In ogni caso, Check Point Software ha recentemente osservato che KillNet affida le istruzioni sugli attacchi DDoS alle masse, forse a causa della mancanza di forza-lavoro necessaria per portare a termine le azioni pianificate e in molteplici occasioni ha offerto ricompense economiche agli affiliati.

Il processo di recruitment è simile per molti gruppi russi. Per esempio, XakNet (che si definisce come il "Team dei Patrioti Russi") è un gruppo di utenti russi attivo all'incirca da marzo 2022. Il gruppo minacciava di contrattaccare per qualunque attacco cyber rivolto contro la Russia e avrebbe individuato diverse entità interne all'Ucraina che hanno rubato dati ufficiali del governo ucraino. XakNet ha dichiarato che non recluteranno hacker, *pentesters* (specialisti nell'esecuzione di test di vulnerabilità di siti web), o specialisti Osint senza esperienza e capacità dimostrate.

Un altro gruppo piuttosto rigido sul reclutamento è quello filorusso di NoName057(16) che investe parte delle sue risorse per offrire un training adeguato ai seguaci tramite canali Telegram, piattaforme di e-learning, tutorial, corsi e attività di mentoring, svolta anche nei canali di supporto in lingua inglese.

I gruppi di hacktivisti si sforzano costantemente di utilizzare strumenti più avanzati per eseguire i loro attacchi, dal momento che più gli attacchi arrecano danni più il gruppo guadagna in termini di notorietà ed esposizione. Nonostante i segnali dell'uso di tecniche avanzate, la maggior parte dell'attività rimane concentrata attorno agli attacchi DDoS tramite il ricorso a enormi botnet (rete di computer zombie sotto il controllo di un'unica entità). Questi attacchi sono tuttavia differenti, suddivisi in attacchi DDoS volumetrici, applicativi

72. Check Point Research 2022.

e infrastrutturali[73], rispetto ai quali non è possibile abbassare la guardia.

7. Conclusioni

Una delle escalation più significative dei vari conflitti che si sono verificati negli ultimi anni può essere identificata come l'attivismo politico nel cyberspazio. Per circa trent'anni, l'hacktivism ha rappresentato un modo per rivendicare il proprio protagonismo, individuale e collettivo, e non sembrava porre rischi significativi alle organizzazioni globali pur provocando danni variamente quantificabili[74]. Oggi, all'inizio degli anni Venti del nuovo secolo, essendo diventato più organizzato, strutturato e sofisticato, l'hacktivism ha inaugurato una nuova era. Solo nel conflitto Russo-Ucraino si contano ben 112 gruppi di hacktivisti che parteggiano per l'una o per l'altra parte in guerra. E i numeri aumentano costantemente. Poiché molti gruppi di hacktivisti hanno un'agenda politica legata agli Stati, questi ultimi potrebbero essere interessati a supportarli in maniera sempre più rilevante e non solo in tempo di guerra.

Il coinvolgimento di attori non statali, il loro utilizzo da parte dei governi, gli attacchi alle infrastrutture civili anche attraverso *ransomware gangs* per attaccare la catena di approvigionamento delle aziende dei paesi alleati coi belligeranti, con l'obbiettivo sia di interferire con la produzione di armi che con l'erogazione di servizi essenziali, sta trasformando Internet in una trincea di guerra. Amaro preludio della fine dell'utopia di un mondo pacifico perché iperconnesso e interdipendente grazie alla Rete.

Riferimenti bibliografici

I. Agrafiotis, J.R.C. Nurse, M. Goldsmith et al. (2018), *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding, how they propagate*, in "Journal of Cybersecurity", vol. 4, 2018, n. 1

J. Assange (2012), *Internet è il nemico. Conversazione con Jacob Appelbaum, Andy Muller-Mauguhn e Jeremie Zimmermann*, Giangiacomo Feltrinelli Editore

Autonome A.f.r.i.k.a. gruppe (a cura di), L. Blisset, S. Brunzels (2001), *Comunicazione-guerriglia. Tattiche di agitazione gioiosa e resistenza ludica all'oppressione*, DeriveApprodi, 2001

F. Berardi Bifo (2011), *La sollevazione. Collasso europeo e prospettive del movimento*, Manni Editori, 2011

H. Bey (2007), *T.A.Z. Zone Temporaneamente Autonome*, ShaKe, 2007; tit. or. *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*, Autonomedia, 1991

J.D. Bolter, R. Grusin (2000), *Remediation: Understanding New Media*, Mit Press, 2000

R.R. Brooks, I. Oxcelik, J. Oakley, N. Tusing (2021), *Distributed Denial of Service (DDoS): A History*, IEEE, 2021

Check Point Research (2022), *The New Era of Hacktivism. State Mobilized Hacktivism Proliferates to the West and Beyond*, 29 September 2022

G. Coleman (2016), *I Mille volti di Anonymous. La vera storia del gruppo hacker più provocatorio al mondo*, Stampa Alternativa, 2016; tit. or. *Hacker, Oaxes, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, 2014

Critical Art Ensemble (1998), *Disobbedienza Civile Elettronica e altre idee impopolari: come sopravvivere e resistere nella società del controllo*, Castelvecchi, 1998; tit or. *Critical Arts Ensemble, Civil Disobedience,* Autonomedia, 1996

73. Csirt Italia 2022.

74. Agrafiotis-Nurse-Goldsmith et al. 2018.

Critical Art Ensemble (1995), *Sabotaggio elettronico. Il primo gruppo americano di critica e attacco ai mass media*, Castelvecchi, 1995

Csirt Italia (2022), *Attacchi DDOS ai danni di soggetti nazionali ed internazionali avvenuti a partire dall'11 Maggio 2022: Analisi e mitigazione*, 13 maggio 2022

A. Curioni, A. Giannuli (2019), *Cyberwar. La guerra prossima ventura*, Mimesis edizioni, 2019

Cyber Infrastructure & Security Agency (2021), *Cyber-Attack Against Ukrainian Critical Infrastructure*, 20 July 2021

D.E. Denning (1999), *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Global Problem Solving Information Technology and Tools, December 10, 1999

M. Deseriis (2017), *Hacktivism, On The use of botnet in Cyberattacks,* in "Theory, Culture and Society", vol. 34, 2017, n. 4

M. Deseriis, G. Marano (2008), *Net.Art. L'arte della connessione*, Shake, 2008

A. Di Corinto (2022), *#OpRussia: Anonymous dichiara guerra a Putin nel cyberspazio*, in "La Repubblica", 4 marzo 2022

A. Di Corinto (2015), *Anonymous minaccia l'Arabia saudita: "Non uccidete Alì"*, in "La Repubblica", 30 settembre 2015

A. Di Corinto (2015a), *Anonymous: "Abbiamo violato la rete jihadista"*, in "La Repubblica", 8 febbraio 2015

A. Di Corinto (2014), *Anonymous ruba gli account del Ku Klux Klan: operazione "Giù il cappuccio", rivelati esponenti*, in "La Repubblica", 18 novembre 2014

A. Di Corinto (2014), *Un dizionario hacker*, Manni Editori, 2014

A. Di Corinto (2010), *Con Wiki, senza amare Julian. Hacker italiani a favore della trasparenza ma non dell'australiano*, in "Il Sole 24 Ore", 14 dicembre 2010

A. Di Corinto (2001), *Don't hate the media, become the media*, in AA.VV., "La sfida al G8", Manifestolibri, 2001

A. Di Corinto, T. Tozzi (2002), *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, 2002

R. Dominguez (2003), *Illegal Knowledge? Strategies for new media activism*, in "Electronic Book Review", 2003

J.D. Downing, T. Villareal Ford, G. Gil, L. Stein (2001), *Radical Media. Rebellious communication and Social Movements*, Sage Publications Inc., 2001

L. Goode (2015), *Anonymous and the Political Ethos of Hacktivism*, in "Popular Communication", vol. 1, 2015, n. 1

A. Greenberg (2019), *Sandworm. A new era of cyberwar and the hunt for Kremlin's most dangerous hackers*, DoubleDay, 2019

N. Klein (2000), *No Logo: Taking Aim at the Brand Bullies*, Picador, 2000

S. Levy (1996), *Hackers, gli eroi della rivoluzione informatica*, ShaKe Edizioni Underground, 1996; tit. or. *Hackers, Heroes of the informatic revolution*, Anchor Press/Doubleday, 1984

Mandiant Intelligence (2022), *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant Intelligence, 2022

F. Massarelli (2011), *La collera della Casbah. Voci di rivoluzione da Tunisi*, Agenzia X, 2011

G. Meikle (2004), *Disobbedienza civile elettronica. Mediattivismo, come costruire una nuova sfera pubblica*, Apogeo, 2004

Microsoft Digital Security Unit (2022), *An overview of Russia's cyberattack activity in Ukraine*, 27 April 2022

L. Ninotti, S. De Tomas Colatin (2022), *Analysis of the Russian-Speaking Threat Actor NoName 057(16)*, 13 October 2022

P. Olson (2012), *We Are Anonymous: Inside the Hacker World of LulzSec*, Little, Brown and Company, 2012

M. Pasquinelli (a cura di) (2002), *Media Activism. Strategie e pratiche della comunicazione indipendente*, DeriveApprodi, 2002

N. Piro (a cura di) (1998), *Cyberterrorismo. Come si organizza un rapimento virtuale*, Castelvecchi, 1998

U. Rapetto, R. Di Nunzio (2001), *Le Nuove Guerre. Dalla Cyberwar ai Black Bloc, dal sabotaggio mediatico a Bin Laden*, RCS Libri, 2001

La Repubblica (2012), *Anonymous attacca la Costituzione "Il popolo deve difendersi dai tiranni"*, 5 marzo 2012

T. Rid (2022), *Misure Attive. Storia segreta della disinformazione*, Luiss University Press, 2022; tit. or. *Active Measures: The Secret History of Disinformation and Political Warfare*, Ferrar Straus & Giroux, 2021

M.N. Schmitt (2017) (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017

Strano Network (1996), *Net strike, no copyright, Et (:- Pratiche antagoniste nell'era telematica*, AAA Edizioni, 1996

A. Tiddi (2002), *Precari. Percorsi di vita tra lavoro e non lavoro*, DeriveApprodi, 2002

T. Tozzi (2019), *Le radici dell'hacktivism in Italia, 1969-1989. Dallo sbarco sulla Luna alla caduta del muro di Berlino*, Accademia di Belle Arti di Firenze, 2019

M. Veneziani (2006), *Controinformazione. Stampa Alternativa e giornalismo d'inchiesta dagli anni Settanta ad oggi*, Castelvecchi, 2006

G. White (2022), *Crime dot com. Il potere globale dell'hacking dai virus ai brogli elettorali,* Odoya, 2022; ed or. *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Globa*, Reaktion publishing, 2020

K. Zetter (2015), *Countdown to zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2015

.Zip!puntozip (1997), *Hot Web. Guida ai siti alternativi e radicali su Internet*, Castelvecchi, 1997

Sitografia

https://t.me/itarmyofukraine2022
https://t.me/itarmyofukraine2022/1637
https://t.me/c/1228309110/34219
https://www.ccc.de/en/
https://web.archive.org/web/20010201081900/http://www.netstrike.it/
http://www.billboardliberation.com/
https://it.wikipedia.org/wiki/Partito_Pirata
https://web.archive.org/web/20120208220331/http://www.rtmark.com/gatt.html
https://web.archive.org/web/*/www.thehacktivist.com

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0124 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Irene Sigismondi

Piattaforme di risoluzione alternativa delle controversie online tra frammentazione di Internet e istanze di giustizia

Il presente lavoro si propone di elaborare alcuni spunti per una riflessione sull'evoluzione degli strumenti di risoluzione delle controversie online (ODR) alla luce delle preoccupanti segnalazioni in relazione alla c.d. frammentazione di Internet, ossia quel fenomeno, denunciato dai fautori della neutralità della rete, che si sta verificando in rete a vari livelli, sia con riguardo all'infrastruttura che ai contenuti e che si ritiene possa mettere in serio pericolo la possibilità di un reale accesso universale e indiscriminato ai servizi offerti in rete. Considerando che la costellazione degli strumenti e piattaforme ODR appartiene al mondo privato, emerge fortemente il rischio che si possano imporre condizionamenti, anche in modo surrettizio, rispetto alla promozione dell'uso e in definitiva all'efficacia deflattiva del ricorso alla giurisdizione pubblica, soprattutto a danno dei soggetti più deboli.

ADR online – ODR-Online dispute resolution – Frammentazione di Internet – Neutralità della rete
Accesso universale – Tutela giurisdizionale

Online dispute resolution platforms between Internet fragmentation and access to justice

The present work is a reflection on the evolution of online dispute resolution (ODR) tools with regards to the emerging worries related to the so-called Internet fragmentation. It is a phenomenon, denounced by supporters of net neutrality, which is occurring online at various levels: both for infrastructure and for content, and it is believed to put in serious danger the actual possibility of universal and indiscriminate access to online services. Considering that the constellation of ODR tools and platforms belongs to the private world, there is a strong risk that conditions could be imposed, even in surreptitious ways, with respect to the promotion of the use and ultimately the effectiveness of the intent to obtain a deflation in access to public justice, especially to the detriment of the weakest subjects.

Online ADR – ODR-Online dispute resolution – Internet fragmentation – Net neutrality – Universal access
Access to justice

L'Autrice è docente al Master in diritto dell'informatica – Dipartimento di scienze giuridiche – Sapienza Università di Roma; *Fellow* presso il *National Center for Technology and Dispute Resolution* (NCTDR) – USA

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Introduzione

Questo articolo[1] si propone di riflettere sul futuro delle piattaforme ODR mettendo in relazione gli elementi tecnici del settore di riferimento, con riguardo più specifico all'area ed al contesto normativo dell'Unione europea, e il dibattito sulla fine di Internet[2], nella sua articolazione particolare rappresentata dalla frammentazione di Internet, sia per gli aspetti di infrastruttura che di esperienza d'uso.

Si tratta di temi che necessariamente devono essere posti in relazione, in quanto il futuro degli strumenti di risoluzione alternativa delle controversie in rete è profondamente legato all'evoluzione della rete stessa, nella sua duplice accezione sia come canale di trasmissione di dati e veicolo di flussi di comunicazione elettronica, sia come web, ossia viaggio ed esperienza di navigazione e, in definitiva, contenuti veicolati, in termini di validità ed efficacia, per usare la stessa terminologia giuridica della teoria generale del diritto con riferimento alla norma.

L'ipotesi che si sostiene, basata su report, dati statistici di tendenza e osservazioni empiriche, è che a fronte di un maggiore utilizzo di Internet, del commercio elettronico e dei servizi in rete, i fenomeni di frammentazione a livello di infrastruttura possono rappresentare un ostacolo al servizio universale, favorendo una gestione in termini asimmetrici dell'accesso alla rete e del traffico. Ciò compromette anche le potenzialità delle piattaforme di risoluzione delle controversie online facendo perdere al tempo stesso una importante opportunità di deflazione dell'accesso alla giurisdizione pubblica, quanto meno per le controversie di minore rilevanza. In altri termini, favorire una migliore esperienza della rete in favore di chi ha a disposizione risorse economiche per garantirsi una "corsia preferenziale" di navigazione può determinare il fallimento anche di questo strumento deflattivo molto importante per la gestione della giustizia.

Sarebbe pertanto necessario preservare il principio di neutralità della rete e l'apertura incondizionata di Internet nella gestione dell'accesso e del traffico dati.

2. La risoluzione alternativa delle controversie online: contesto di riferimento

ODR è un acronimo che sta per *Online Dispute Resolution* e sottintende anche un riferimento a sistemi ovvero tecnologie, da intendersi come tutti gli strumenti per la risoluzione alternativa delle controversie che possono essere predisposti, approntati e fruiti con la tecnologia informatica e telematica ossia anche utilizzando la rete.

Senza entrare nel dettaglio dal punto di vista processual-civilistico, la sua derivazione dall'ampia famiglia della risoluzione alternativa delle controversie colloca questo concetto, e i suoi annessi e connessi tecnologici, nell'alveo delle ADR, ossia

1. Ringrazio i Curatori per aver ospitato questo lavoro che si presenta ancora in fase di sviluppo, frutto di riflessioni ed elaborazioni preliminari risultato anche della collaborazione all'interno del NCTDR. Sono tuttavia la sola responsabile delle opinioni espresse in questo contributo, che non rappresentano il NCTDR o i suoi membri e partner.
2. Per una visione d'insieme al dibattito sulla c.d. "fine di Internet" si fa riferimento a questa Sezione monografica, che fornisce anche validi riferimenti e spunti specifici in diversi settori.

i modi di risoluzione alternativa delle controversie. Tuttavia, la classificazione è articolata, proprio come per le ADR nella previsione di sottogruppi, quali la negoziazione, la mediazione o l'arbitrato o anche combinazioni dei tre strumenti, a seconda del grado di influenza che l'intervento umano di un terzo può avere nel processo di ricerca di una soluzione. L'uso della tecnologia informatica e lo svolgimento con mezzi telematici di tutto il processo di ricerca della soluzione sono sicuramente i connotati più specifici di una modalità che rappresenta una innovazione che potrebbe favorire, anche nell'intento del legislatore europeo, la riduzione dell'accesso alla giustizia, inteso come riferimento ai sistemi tradizionali della giurisdizione, peraltro, sempre nel rispetto dei principi costituzionali di inderogabilità.

Sotto il profilo normativo, la disciplina in Europa è significativamente affidata al Regolamento 524/2013[3], mentre per la tradizionale ADR, la fonte di riferimento è la Direttiva 2013/11/UE[4]. Questa distinzione, anche se le fonti sono state adottate in stretto coordinamento, fa subito emergere la necessità stringente di legare l'ODR ad una standardizzazione ed uniformità, laddove invece per l'ADR è lasciata agli Stati quella discrezionalità attuativa per consentire il pieno rispetto dei principi costituzionali degli Stati, pur nel quadro comune degli obiettivi da perseguire posti dalla Direttiva.

La piattaforma ODR messa in campo dall'Unione europea è soltanto una di quelle disponibili in rete globalmente ed il mercato mostra un potenziale considerevole, in quanto potrebbe attrarre al settore privato un numero elevato di controversie caratterizzate da una precisa configurazione qualitativa e quantitativa: si tratta infatti di controversie di numero elevato (*high volume*), ma di basso rilievo considerate singolarmente (*low value*).

Questi parametri sono stati a lungo al centro della complessa opera di drafting normativo del Working Group III dell'UNCITRAL (Commissione delle Nazioni Unite per il diritto commerciale internazionale)[5] durante le sessioni di lavoro del 2010-2011, poi riprese conclusivamente nel 2016 con due documenti: Bozza di documento finale che riflette elementi e principi di un processo ODR[6] e Note Tecniche sull'*Online Dispute Resolution*[7]. A livello transnazionale, si tratta di un tema di grande interesse, in quanto manca uno strumento normativo cogente che garantisca la tutela dei diritti al di fuori dei casi già codificati dal diritto internazionale privato. La giurisdizione, infatti, è fortemente legata alla sovranità ed al territorio e ciò rende difficile intervenire nelle controversie tra privati, specie quando l'elemento geografico è vago o ambiguo, rispetto ai criteri normativi tradizionali, come accade per le dispute che nascono in ambito Internet. Il delicato profilo diplomatico che sta dietro i documenti dell'UNCITRAL sta proprio nella ricerca di elementi di standardizzazione che rendano possibile agli Stati di affrontare i temi della tutela giurisdizionale in modo uniforme e garantire che le controversie transnazionali possano rispondere a criteri comuni quando si tratta di aprire una procedura di ODR. Si tratta delle definizioni normative di principi, fasi, obiettivi e procedura, con una codificazione comune di tutte le garanzie da approntare nei singoli Stati.

In Europa, come si è detto, tutto è affidato al Regolamento ODR, che prevede la disciplina della procedura e le varie fasi ed al successivo Regolamento di implementazione[8].

3. Regolamento (UE) n. 524/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo alla risoluzione delle controversie online dei consumatori e che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (regolamento sull'ODR per i consumatori).
4. Direttiva 2013/11/UE del Parlamento europeo e del Consiglio, del 21 maggio 2013, sulla risoluzione alternativa delle controversie dei consumatori, che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (direttiva sull'ADR per i consumatori).
5. Per i lavori del WGIII in materia di ODR, v. United Nations 2010-2016 e United Nations 2017.
6. V. United Nations 2015. Il documento significativamente riguarda una definizione condivisa tra gli Stati sugli elementi standard di un processo di ODR, ma non la natura o l'efficacia della sua fase conclusiva in caso di successo.
7. Si tratta delle *Technical Notes on Online Dispute Resolution*, cfr. United Nations 2017.
8. Regolamento di esecuzione (UE) 2015/1051 della Commissione, del 1° luglio 2015, relativo alle modalità per l'esercizio delle funzioni della piattaforma di risoluzione delle controversie online, alle caratteristiche del modulo

La piattaforma europea di risoluzione delle controversie online (ODR) è gestita dalla Commissione europea nell'ambito degli obiettivi di rafforzamento della fiducia verso il commercio elettronico e prevede che il consumatore effettui una richiesta ad un fornitore di beni o servizi online che viene contattato dalla piattaforma. È possibile formulare una richiesta/reclamo sul punto di accesso determinato dal sito della piattaforma ODR, allegando documenti ed anche, eventualmente, richiedendo un incontro con il fornitore di beni o servizi online. Nel termine di 90 giorni è possibile raggiungere un accordo, ma resta sempre aperta la possibilità di ritirarsi dai contatti diretti in qualsiasi momento. Il fornitore di beni o servizi online può proporre un elenco di organismi di risoluzione delle controversie a cui rivolgersi invece di trovare direttamente una soluzione ed in tal caso il termine per concordare l'organismo è di 30 giorni, diversamente il caso viene chiuso. In caso di rifiuto o ritiro dalle trattative si può comunque chiedere l'intervento di un organismo di risoluzione delle controversie approvato. In caso di fallimento, si può ricorrere ad altri strumenti quali i centri europei o gli organismi nazionali per la tutela dei consumatori, la rete FIN-NET per le controversie di natura finanziaria, le procedure di *Small Claims* con l'ordine di pagamento europeo ed organismi per la risoluzione delle controversie accreditati presso la Commissione.

3. Le piattaforme di risoluzione alternativa delle controversie online: dati di utilizzo

La specifica connotazione dell'ODR, quale risoluzione delle controversie online, è sicuramente l'utilizzo dell'infrastruttura tecnologica che fornisce gli strumenti per la gestione della questione: in altri termini è necessaria un'infrastruttura che consenta l'esplicazione delle potenzialità di dialogo tra le parti, con o senza l'intervento umano, come dalle possibili articolazioni che sono state accennate sopra.

Il maggiore *appeal* di una simile modalità è sicuramente legato al mondo della rete ed ai servizi informatici e telematici che più facilmente potrebbero giovarsi di strumenti di questo tipo, per ragioni oggettive e soggettive[9].

Da una parte, infatti, al crescere della presenza in rete delle imprese in Europa[10] e del commercio elettronico in Italia[11] si prospetta un naturale percorso di soluzione di eventuali controversie sorte in relazione al contratto nel canale digitale, che renderebbe semplice – anche se non sempre facile – adottare la decisione di prediligere uno strumento agile, disponibile in rete, dai costi accessibili e senza la necessità di intermediazione legale professionale.

Dall'altra, i soggetti che effettuano acquisti in rete mostrano una preferenza per l'utilizzo della rete anche per esercitare i propri diritti di consumatori in caso di necessità.

di reclamo elettronico e alle modalità della cooperazione tra i punti di contatto di cui al regolamento (UE) n. 524/2013 del Parlamento europeo e del Consiglio relativo alla risoluzione delle controversie online dei consumatori.

9. La Commissione ha effettuato nel tempo numerosi studi per dare la maggior rilevanza possibile alla piattaforma ODR. Si veda la pagina di riferimento su studi e ricerche in tema di ODR.
10. L'Annuario Statistico 2022 (aggiornato al dicembre 2022) riferisce che nel 2021 il 78,0 per cento delle imprese europee era presente sul web con una propria home page, precisando che il divario tra il paese con la maggiore quota di imprese on line e quello con la più bassa rimane elevato, pari a circa 45 punti percentuali. Rispetto a questo dato, le imprese della Finlandia, dei Paesi Bassi e dell'Austria sono quelle più presenti sul web (rispettivamente 96, 92 e 91 per cento), mentre si registrano in Portogallo, Bulgaria e Romania le quote più basse di imprese con sito internet (rispettivamente 62, 52 e 51 per cento). L'Italia si collocava al 14° posto. Cfr. ISTAT 2022.
11. Sempre facendo riferimento all'ASI, tra i macrosettori, quello dei servizi risulta il più attivo nelle vendite on line (24,2%), con una quota notevole di imprese che vende via web tramite siti web o app dell'impresa (71,5%), anche se è l'industria manifatturiera il settore che utilizza maggiormente questo canale con il 79,4% di imprese. Le imprese più attive nelle vendite elettroniche sono quelle delle attività di alloggi (83,7%), delle attività editoriali (73,1%) e delle telecomunicazioni (30,1%). Cfr. ISTAT 2022, p. 767.

Per consentire un confronto tra il dato del commercio elettronico e quello della piattaforma ODR in UE è utile prendere in considerazione il report pubblicato di recente dalla Commissione europea per l'aggiornamento quadriennale della situazione in relazione all'uso di ADR e ODR[12].

Ebbene, i dati che emergono sono significativi di una situazione di stallo: il report segnala infatti che l'interesse dei consumatori nei confronti della piattaforma è tutto sommato limitato e le richieste di attivazione della procedura nei riguardi degli esercenti commercio elettronico hanno sortito un effetto nullo, rimanendo inascoltate nella maggior parte dei casi, o hanno visto controproposte di risoluzione dei casi al di fuori della piattaforma. In conseguenza di ciò si registra che soltanto intorno al 2% delle richieste di attivazione sono state effettivamente inviate ad un organismo accreditato per l'effettivo svolgimento della procedura come prevista dal Regolamento.

Proprio nella stessa data di produzione del report, Il 17 ottobre 2023, la Commissione europea ha adottato una proposta di revisione del quadro ADR composto di tre passaggi: la modifica della Direttiva ADR[13], una Raccomandazione sui requisiti di qualità per le procedure di risoluzione delle controversie offerte dai mercati online e dalle associazioni di categoria dell'Unione[14] e soprattutto, per quanto qui di interesse, l'abrogazione del Regolamento ODR[15].

Ebbene, nelle premesse della proposta di abrogazione, si riferisce che nonostante abbia un numero elevato di visite, la piattaforma ODR in media in tutta l'UE risolve soltanto 200 casi trattati da un organismo ADR all'anno.

La Commissione sostiene che questo livello di prestazioni non giustifica i costi sostenuti dalla Commissione per il mantenimento dello strumento, né il costo sostenuto dalle pubbliche amministrazioni e dalle imprese online per conformarsi alle previsioni del regolamento ODR. Si prevede quindi di abrogare il Regolamento ODR, dismettendo così la piattaforma ODR e rimuovendo di conseguenza anche l'obbligo per le attività online di fornire un collegamento alla piattaforma ODR e gestire con una mail dedicata le relative comunicazioni.

Il report attribuisce gli scarsi risultati della piattaforma ODR alla mancanza di informazione su come funziona l'ADR, al disinteresse dei fornitori di beni e servizi online ed alla difficoltà dei consumatori nel compilare i reclami in relazione ai criteri minimi di ammissibilità fissati dagli organismi di ADR.

Si tratta di una sconfitta del modello online? Alla luce di quanto appena rilevato, probabilmente la piattaforma ODR non è stata costruita secondo i principi di semplificazione e "digital first" di cui al nostro Codice dell'Amministrazione Digitale perché non ha colmato lo spazio di libertà delle parti, determinando così troppo spesso l'inerzia o il fallimento delle procedure nella fase embrionale di attivazione. Tuttavia, forse, vi è anche un tema legato all'accesso alla piattaforma che si lega più squisitamente al profilo tecnico e di questo cercheremo di dare una rappresentazione nel prossimo paragrafo: si tratta della frammentazione di Internet e di tutto quel variegato e complesso fenomeno di criticità che incontra il principio di neutralità della rete e apertura di Internet.

4. Il dibattito sulla frammentazione di Internet

L'espressione "Internet Fragmentation" ha una connotazione politica legata alla governance di Internet, è stata utilizzata per la prima volta durante il *World*

12. Si tratta del *Report on the application of Directive 2013/11/EU on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013*, COM(2023) 648 final, 17 ottobre 2023.
13. Cfr. Proposta di Direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2013/11/UE sulla risoluzione alternativa delle controversie dei consumatori e le direttive (UE) 2015/2302, (UE) 2019/2161 e (UE) 2020/1828, doc. COM(2023) 649 del 17 ottobre 2023.
14. Cfr. Raccomandazione (UE) 2023/2211 della Commissione del 17 ottobre 2023 sui requisiti di qualità per le procedure di risoluzione delle controversie offerte dai mercati online e dalle associazioni di categoria dell'Unione.
15. Cfr. Proposta di Regolamento del Parlamento europeo e del Consiglio che abroga il regolamento (UE) n. 524/2013 e modifica i regolamenti (UE) 2017/2394 e (UE) 2018/1724 per quanto riguarda la dismissione della piattaforma europea ODR, doc. COM(2023) 647, del 17 ottobre 2023.

Economic Forum del 2015[16] e sta a rappresentare un fenomeno di dispersione, divisione, frammentazione appunto, che riguarda diverse dimensioni (*realm*), e si esplica variamente impattando su aspetti tecnici, di governo e commerciali, così come vengono in essere all'interno della rete[17].

Se si vuole semplificare, per dare un quadro della situazione, frammentare significa parcellizzare, atomizzare, disperdere il segnale e quindi per un verso (tecnico) diminuire la qualità della navigazione, per un altro creare un'esperienza di navigazione inceppata e difficoltosa (user experience) e per un altro ancora subire influenze commerciali nella distinzione dei servizi offerti in rete, sulla base di criteri economici e remunerativi, anziché legati alla tipologia di servizi.

In altri termini, mettere in discussione la neutralità della rete come mero strumento di veicolazione di dati a prescindere da profili soggettivi (chi si connette) e oggettivi (natura dei dati).

Si tratta di un tema assai delicato, che è stato ricollegato alla globalizzazione ed ai suoi effetti positivi e negativi sullo sviluppo[18]. Paradossalmente, la fragilità dell'attuale panorama geopolitico rende Internet globale una "minaccia" per i particolarismi, per la ri-frammentazione dello scacchiere internazionale sotto il profilo dei nazionalismi. Se è vero che a livello dei contenuti già sussistono limitazioni dal momento che non tutti i contenuti sono disponibili per tutti e dappertutto, per ragioni di controllo a vari livelli (si pensi ad esempio alle funzionalità previste per il controllo parentale), è anche vero che non si tratta di frammentazione in senso proprio. La frammentazione si può collegare alla mancanza di interoperabilità: idealmente manca il passaggio da un segmento all'altro della rete e viene così meno la comunicazione e il contenuto non viene veicolato. Questo determina una parcellizzazione delle conoscenze ed una perdita secca in relazione alla società della conoscenza, perché non c'è più accesso pieno ed incondizionato alla rete ed ai dati.

5. Alcune riflessioni in prospettiva

Risulta molto complesso effettuare una proiezione dei dati attuali sull'utilizzo della rete per il commercio elettronico e gli altri servizi presenti per poter fare un pronostico in ordine al possibile successo di nuove piattaforme di ODR ed al reale impatto dei fenomeni di frammentazione di Internet a livello pubblico e privato. Infatti, non si può tracciare una linea in continuità con la tendenza registrata, dal momento che metodologicamente abbiamo imparato che eventi di impatto globale come la pandemia e le guerre, accaduti e tutt'ora in atto a partire dagli ultimi tre anni, sono in grado di modificare le priorità delle politiche pubbliche ed anche il sistema di preferenze degli utenti privati e le loro abitudini di consumo in rete.

Ciò non toglie che sia di fondamentale importanza far conoscere e tenere alta l'attenzione dell'opinione pubblica sui temi legati alla frammentazione di Internet, che possono far cambiare la natura stessa della rete come l'abbiamo conosciuta fino ad ora.

L'educazione al digitale, lo sviluppo di servizi in rete anche da parte delle amministrazioni pubbliche nella logica della semplificazione e del "digital first" possono aiutare a far convergere gli sforzi verso una migliore gestione della rete da parte dei privati, accompagnati nell'individuare le modalità di utilizzo di servizi chiave, come può essere una piattaforma per l'ODR.

Il dichiarato fallimento della piattaforma unica per l'ODR gestita in Europa che ne preannuncia la chiusura ed abrogazione della normativa di riferimento si traduce in una perdita secca con riferimento alla cultura digitale e determina altresì un forte rallentamento in relazione alle reali possibilità di ottenere gli effetti deflattivi del contenzioso civile nei sistemi di giurisdizione tradizionale attraverso il ricorso a canali e mezzi alternativi, soprattutto per quanto riguarda le controversie di minor valore e però di impatto consistente e ricorrente nelle relazioni commerciali e tra privati nella vita quotidiana, con ricadute negative soprattutto verso coloro che hanno minori risorse.

16. Cfr. il *Report* pubblicato nel sito web del World Economic Forum e la successiva nota 16.
17. Per una attenta ricostruzione dei vari profili interessati da queste problematiche si veda Drake-Cerf-Kleinwächter 2016.
18. Molto acutamente cfr. Mueller 2017.

Riferimenti bibliografici

Istat (2022), *Annuario Statistico Italiano*, 2022

W.J. Drake, V.G. Cerf, W. Kleinwächter (eds.) (2016), *Future of the Internet Initiative White Paper - Internet Fragmentation: An Overview*, 2016

M. Mueller (2017), *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*, Digital Futures, John Wiley & Sons, 2017

United Nations - Commission On International Trade Law (2010-2016), *Online dispute resolution (2010-2016) working documents*

United Nations (2015), *Draft outcome document reflecting elements and principles of an ODR process*, 2015

United Nations (2017), *Technical Notes on Online Dispute Resolution*, 2017

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0122 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Elia Cremona

Quando i dati diventano beni comuni: modelli di *data sharing* e prospettive di riuso

La regolazione europea in materia di dati sembra cambiare paradigma: l'enfasi non è più solo sul profilo della *protezione* e del *controllo*, ma anche della *condivisione*. In questa direzione vanno, in particolare, il *Data Governance Act* e il *Data Act*. Il primo, infatti, promuove il riutilizzo di dati protetti detenuti da enti pubblici, l'intermediazione e il c.d. altruismo dei dati. Il secondo si incentra sui temi dell'accesso ai dati, del diritto di condividere i dati con i terzi e infine sull'obbligo di mettere i dati di soggetti privati a disposizione di enti pubblici per necessità eccezionali. Insomma, la nuova stagione regolatoria europea libera nuovi flussi di dati tra settore pubblico e settore privato (*Business to Government* e *Government to Business*). Il contributo propone una rilettura in chiave critica di tali normative e promuove l'idea dei *data for common good*: un regime speciale per i dati detenuti da soggetti privati ma di pubblico interesse, che vada ad integrare le policy di sostenibilità sociale delle grandi imprese.

Data sharing – Beni comuni – Riuso dei dati – Sostenibilità

When Data Become Commons: Models of Data Sharing and Re-use Perspectives

European data regulation is changing paradigm: the emphasis is no longer only on the profile of protection and control, but also on sharing. In this direction go, in particular, the Data Governance Act and the Data Act. The former, in fact, promotes the reuse of protected data held by public entities, intermediation and so-called altruism of data. The latter focuses on the issues of data access, the right to share data with third parties, and finally the obligation to make data from private entities available to public entities for exceptional needs. In short, the new European regulatory season frees up new data flows between public and private sectors (Business to Government and Government to Business). The paper proposes a critical reinterpretation of these regulations and promotes the idea of data for common good: a special regime for data held by private entities but in the public interest, complementing the social sustainability policies of large companies.

Data sharing – Commons – Data Re-use – Sustainability

L'Autore è assegnista di ricerca in Diritto costituzionale nell'Università degli Studi di Siena

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Le stagioni della regolazione dei dati: proprietà, controllo, condivisione

Quando Samuel D. Warren e Louis Brandeis si inventarono il diritto alla privacy[1], inteso – com'è ampiamente noto – nel senso di "right to be let alone", avevano in mente le intrusioni nella vita privata da parte della neonata stampa scandalistica, accusata da parte loro di aver varcato i limiti della decenza e del rispetto del diritto di proprietà[2]. Il diritto alla privacy veniva così coniato come "espansione" del più sacro dei diritti dello stato liberale: la proprietà, appunto, non più considerata come dominio sulle cose connotate da materialità, ma estesa al diritto di impedire la divulgazione di informazioni, pensieri e sentimenti riferibili al soggetto interessato.

Oggi, se pure l'etichetta privacy sia sopravvissuta e ancora largamente impiegata anche nel comune dibattito pubblico, è rimasto ben poco del "diritto ad essere lasciati soli". Anzi, il principale campo di applicazione della normativa c.d. privacy è quello delle relazioni sociali nello spazio digitale, nel quale l'*animus* dell'utente medio è non già quello di escludere qualcuno dal proprio dominio (*excludendi*) bensì di condividere (*communicandi*) informazioni, pensieri e sentimenti che lo riguardano con una platea più ampia possibile di soggetti. Ciò si verifica sia nell'ipotesi in cui la condivisione del dato è lo scopo diretto dell'utente sul web, come nel caso delle piattaforme social (*Instagram*, *X*, *Facebook*), sia quando la condivisione è invece strumentale all'accesso ad un servizio, come nel caso dei servizi "gratuiti" di cui fruiamo quotidianamente attraverso internet (dalla galassia dei servizi Google ai software Microsoft, fino ai più recenti sistemi di intelligenza artificiale generativa come *Chat-GPT*): per quanto il grado di consapevolezza medio dell'effetto "sorveglianza" che questa fruizione gratuita produce sia ancora molto scarso, soprattutto nelle generazioni più giovani, non si può dubitare del fatto che nello spazio digitale la privacy, tradizionalmente intesa, sia divenuta un problema recessivo[3].

1. Il riferimento è al noto Warren-Brandeis 1890, pp. 193-220.
2. *Ivi*, p. 196: «the press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and the vicious, but has become a trade. […] To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers».
3. Sull'alternativa tra pagamento di un prezzo e cessione dei dati personali, si veda la recente decisione di Meta di sottoporre la scelta ai propri utenti europei. A fine ottobre 2023, infatti, è comparso sugli schermi degli utenti questo avviso: «Per ottemperare alle normative europee in continua evoluzione stiamo introducendo la possibilità di sottoscrivere un abbonamento in Ue, See e in Svizzera. A novembre offriremo alle persone che utilizzano Facebook o Instagram che risiedono in queste regioni la possibilità di continuare a utilizzare questi servizi personalizzati gratuitamente con la pubblicità, oppure di sottoscrivere un abbonamento per non visualizzare

L'evoluzione dei costumi sociali è così "ruotata" intorno al concetto di privacy, che sul piano giuridico è però rimasto per lungo tempo ancorato alla cultura proprietaria che lo aveva ispirato.

Volendo scandire le tappe essenziali di questo percorso di affrancamento dal modello proprietario, possiamo – sul piano costituzionale e del diritto europeo – indicare questa sequenza di atti: la Convenzione Europea dei Diritti dell'Uomo, la Direttiva 95/46/CE, la Carta di Nizza, il GDPR e, da ultimo, il corposo pacchetto di atti con i quali l'Unione europea ha disciplinato il fenomeno digitale.

In via di sintesi: il citato modello proprietario ha prodotto sul piano normativo l'affermazione del diritto al rispetto della vita privata e familiare, postulato in ambito convenzionale dall'art. 8 della CEDU e ribadito all'art. 7 della Carta di Nizza. A questo si è affiancato, dapprima con la Direttiva 95/46/CE[4], poi con l'art. 8 della Carta di Nizza, l'art. 16 del TFUE e infine con il GDPR, il paradigma del "controllo" e della "protezione dei dati", non più inteso in senso assolutistico quale proiezione di un diritto di proprietà, ma quale punto di caduta del bilanciamento tra l'esigenza di tutelare un diritto fondamentale della personalità con l'opposta esigenza di garantire quanto più possibile la "circolazione" dei dati, personali e non personali.

Diversamente dalla comune vulgata[5], il GDPR ha sin da subito rappresentato un compromesso

più le inserzioni. Le informazioni delle persone che decideranno di sottoscrivere l'abbonamento non saranno utilizzate per gli annunci pubblicitari. […] A seconda che si scelga di attivare l'abbonamento sul web o da mobile il costo sarà rispettivamente di 9,99 euro al mese sul web o di 12,99 euro al mese su iOS e Android». La conformazione dell'avviso suggeriva, con la solita tecnica di *nudging* consistente in una colorazione più *catchy* del relativo bottone, la scelta per il servizio gratuito. Ciò a dimostrazione del fatto che Meta non ha alcuna intenzione di cambiare il proprio *business model*. Questa mossa è stata in realtà la risposta alla decisione, urgente e vincolante *ex* art. 66 GDPR, adottata il 27 ottobre 2023 dall'*European Data Protection Board* (EDPB) che aveva imposto di acquisire il consenso degli utenti per il c.d. *behavioural advertising*. A questa è seguita, il 10 novembre 2023, la decisione finale dell'Autorità irlandese che ha conseguentemente imposto il divieto di trattamento. Nelle due settimane intercorrenti tra i due provvedimenti, però, Meta aveva già sottoposto a tutti i propri utenti europei la scelta tra consenso al trattamento per fini di pubblicità comportamentale e pagamento di un prezzo. Non è irragionevole pensare che la percentuale di coloro che hanno scelto di abbonarsi sia risibile e che dunque, nell'arco di qualche giorno, Meta possa avere acquisito il consenso di qualche centinaio di milioni di persone. Non è questa la sede per ulteriori approfondimenti, ma due osservazioni possono farsi sin d'ora. La prima è che la modalità di acquisizione del consenso da parte di Meta si è rivelata particolarmente aggressiva: l'utente si è trovato improvvisamente a dover scegliere tra dare il consenso e pagare una somma di oltre 100 € all'anno, molto rilevante per il mercato di riferimento (le altre piattaforme social sono quasi tutte gratuite, mentre per X si parla dell'introduzione di un abbonamento di 1 dollaro all'anno). Questo può far pensare sia ad un possibile illecito antitrust, sulla falsariga di quello sanzionato dal *Bundeskartellamt* per illegittima compressione della libertà di scelta del consumatore (*fehlende Wahlmöglichkeit*), sia ad una possibile pratica commerciale scorretta, forse pure di tipo aggressivo. Sulla vicenda tedesca, si veda Pardolesi-Van den Bergh-Weber 2020, pp. 518-519; Davola 2021, p. 65. Le impugnazioni in sede giudiziaria del provvedimento hanno occasionato, com'è noto, l'importante sentenza CGUE, 4 luglio 2023, in causa C-252/21, *Meta platforms e a.* (condizioni generali d'uso di un social network), ECLI:EU:C:2023:537. Per un commento, v. Bachelet 2023. La seconda considerazione che può accennarsi è poi di carattere generale: la velocità – e la facilità – con la quale Meta ha formalmente ottemperato al parere vincolante dell'EDPB, di nuovo grazie al consenso (dis)informato degli utenti, dimostra ancora una volta la debolezza della regolazione europea di fronte allo strapotere – di fatto – delle grandi piattaforme nello spazio digitale. Anzi, recuperando le intuizioni di Pistor 2019, quel che emerge è piuttosto l'uso della legislazione proprio come strumento di consolidamento del potere di queste grandi piattaforme digitali. Cfr. in tema Sandulli 2021.

4. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
5. Cfr. Commissione europea 2020.

tra le esigenze del mercato dei dati e quello della tutela dei diritti[6], delineando uno statuto giuridico dei dati personali per lo più *funzionale* al consolidamento e al corretto funzionamento del mercato unico e, solo in parte, *strumentale* alla garanzia delle libertà fondamentali dell'Unione[7].

Dopodiché, il processo non si è arrestato e il concetto giuridico di "dato" ha iniziato a "spersonalizzarsi", in un'ottica sempre più funzionale all'integrazione del mercato unico[8]. A partire dal 2017, l'Unione ha avviato un ampio processo di riforma che si è incentrato sul tema dell'apertura dei dati e il riutilizzo delle informazioni del settore pubblico (flussi *Government to Government*, c.d. G2G, e *Government to Business*, c.d. G2B)[9]. Dopodiché, le tappe sono state scandite dall'approvazione, nel 2018, del Regolamento sulla circolazione dei dati non personali[10] e poi dalla pubblicazione della *Strategia europea per i dati* del febbraio 2020[11], che ha gettato le basi, tra gli altri, per il *Data Governance Act*[12] (che per primo definisce il "dato" in quanto tale[13]) e il *Data Act*[14]. In particolare, l'Unione ha annunciato la creazione di spazi comuni europei di dati[15] in alcuni settori strategici[16], non rinunciando ad incoraggiare – ed è questo il profilo su cui ci si soffermerà in chiusura – lo sblocco di flussi di dati dal settore privato a quello pubblico (*Business to Government*,

6. Si è sostenuto altrove che tale compromesso si è risolto forse più a vantaggio dei protagonisti dei mercati digitali che degli utenti, spesso inconsapevoli sia della compressione dei propri diritti riconosciuti dal GDPR che degli strumenti di tutela, largamente inattivati. Cfr. Cremona 2023, p. 105 ss.
7. Cfr. De Gregorio-Paolucci 2022, p. 113. Tale profilo emerge abbastanza chiaramente già dai considerando della Direttiva del 1995, ma anche dalla Direttiva 2000/31/EC relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").
8. Cfr. Zech 2015, p. 192; De Franceschi-Lehmann 2015.
9. Tale processo ha condotto all'adozione della Direttiva UE 2019/1024, c.d. Direttiva *Open Data*. Nel 2017, infatti, la Commissione europea aveva aperto una consultazione pubblica sulla revisione della direttiva 2013/37/UE, che a sua volta aveva modificato la direttiva 2003/98/CE in tema *Public Sector Information*.
10. 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. Cfr. Galiano-Leogrande-Massari-Massaro 2020, p. 63.
11. Commissione europea, *Una strategia europea per i dati*, COM(2020) 66, del 19 febbraio 2020. Cfr. anche European Data Protection Supervisor 2020, p. 4.
12. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724.
13. Ai sensi dell'art. 2, par. 1, n. 1), del *Data Governance Act* appartiene alla definizione di dati «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».
14. Al momento in cui si scrive, il *Data Act* è stato definitivamente approvato ed è in attesa di pubblicazione sulla Gazzetta Ufficiale dell'Unione europea.
15. Gli spazi comuni europei dei dati riuniscono le infrastrutture di dati e i quadri di governance pertinenti al fine di facilitare la messa in comune e la condivisione dei dati. In particolare essi (i) implementano strumenti e servizi di condivisione dei dati per la raccolta, l'elaborazione e la condivisione dei dati da parte di un numero aperto di organizzazioni e uniscono capacità *cloud* efficienti dal punto di vista energetico e affidabili e servizi correlati; (ii) includono strutture di governance dei dati, compatibili con la pertinente legislazione dell'Ue, che determinano, in modo trasparente ed equo, i diritti di accesso e trattamento dei dati; (iii) migliorano la disponibilità, la qualità e l'interoperabilità dei dati, sia in contesti specifici che tra settori diversi. V. Commissione europea, *Commission staff working document on Common European Data Spaces*, SWD(2022) 45 final, 23 February 2022.
16. Sanità, agricoltura, manifattura, energia, mobilità, finanza, pubblica amministrazione, competenze, *cloud* europeo per la scienza aperta e soddisfacimento degli obiettivi del Green Deal. A questi si sono poi aggiunti altri settori importanti come quello dei media e del patrimonio culturale. L'obiettivo finale perseguito è che, insieme, gli spazi di dati formino uno spazio unico europeo, un vero mercato unico dei dati.

c.d. B2G)[17] e tra privati (*Business to Business*, c.d. B2B, e *Business to Consumer*, c.d. B2C)[18].

Dunque, quel che si va verificando nelle pagine seguenti è se non sia appena stato compiuto, nel campo regolatorio europeo, un passo *definitivo* nel processo di allontanamento dal paradigma proprietario che ha caratterizzato la prima (*right to be let alone*) e, in parte, la seconda stagione (*protezione e controllo*) della normativa privacy. In particolare, ci si chiederà se non siamo entrati in una (terza) fase regolatoria caratterizzata da un accento sul tema della "condivisione"[19], che mira a "liberare" enormi quantità di dati a beneficio del mercato unico e, auspicabilmente, anche della collettività.

2. Il riutilizzo dei dati del settore pubblico

La presa di consapevolezza sulle potenzialità derivanti dalla condivisione dei dati ha come primo punto di emersione, come si accennava, la previsione di una disciplina di apertura dei dati e riuso delle informazioni del settore *pubblico*. Questo, come vedremo, si spiega secondo una logica molto semplice: mentre i dati del settore privato costituiscono generalmente un *asset* patrimoniale strumentale all'esercizio dell'attività d'impresa, secondo le logiche della concorrenza e della rivalità, viceversa i dati nella disponibilità dei soggetti pubblici non soggiacciono – di norma – a logiche di mercato. In altre parole, se la condivisione e il riuso dei dati nel settore privato si scontrano con le dinamiche dei vantaggi e degli svantaggi competitivi, nel settore pubblico la stessa operazione di "messa a disposizione" dei dati a soggetti terzi (pubblici o anche privati) assume i contorni di una esternalità positiva, ovvero di una azione non specificamente remunerata che produce di per sé effetti positivi sull'economia o sull'attività di altri soggetti.

2.1. La Direttiva *Open Data*

Esattamente a questa logica è ispirata la Direttiva *Open Data* 2019/1024[20] che ha stabilito le regole per l'accesso e l'utilizzo dei dati pubblici da parte delle organizzazioni pubbliche e private all'interno dell'Ue. La direttiva muove da alcune considerazioni che è qui utile riproporre: «il *settore pubblico* degli Stati membri *raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni* in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione. […] La *fornitura di tali informazioni* […] consente ai cittadini e alle persone giuridiche di *individuare nuovi modi di utilizzarle e di creare prodotti e servizi nuovi e innovativi*»[21]. E ancora più chiaramente: «*l'informazione del settore pubblico* rappresenta una fonte straordinaria di dati *in grado di contribuire a migliorare il mercato interno e lo sviluppo di nuove applicazioni per i consumatori e le persone giuridiche*. L'utilizzo intelligente dei dati, ivi compreso il loro trattamento attraverso applicazioni di intelligenza artificiale, può *trasformare tutti i settori dell'economia*»[22].

Per conseguenza, la direttiva fissa un *Principio generale* (art. 3) per il quale i "documenti" in possesso di enti pubblici e imprese pubbliche siano riutilizzabili «a fini commerciali o non commerciali»[23],

17. Commissione europea 2020.
18. Commissione europea 2019.
19. Il concetto di condivisione, come si vedrà *infra*, va distinto dalla mera circolazione. Sebbene non vi sia una definizione di "circolazione" nel GDPR, questa si differenzia dalla "condivisione", definita come segue all'art. 2, par. 1, n. 10), del Regolamento UE 2022/868 (*Data Governance Act*): «la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».
20. La Direttiva *Open Data* dell'Unione europea (EU) 2019/1024 è stata recepita in Italia dal d.lgs. n. 200/2021 che ha emendato il d.lgs. 36/2006.
21. Considerando n. 8, nostro il corsivo.
22. Considerando n. 9, nostro il corsivo.
23. Art. 3 (*Principio generale)*: «1. Fatto salvo il paragrafo 2 del presente articolo, gli Stati membri provvedono affinché i documenti cui si applica la presente direttiva in conformità dell'articolo 1 siano riutilizzabili a fini

siano messi a disposizione in un «lasso di tempo ragionevole» (art. 4)[24] a titolo, di regola, gratuito (art. 6)[25], sempre salvo il rispetto della normativa in materia di protezione dei dati personali, di diritto d'autore e di proprietà industriale.

2.2. Il profilo pubblicistico del *Data Governance Act*

Con il *Data Governance Act*[26], definitivamente applicabile nell'Unione dal 24 settembre 2023, la logica del riutilizzo dei dati pubblici viene ulteriormente sviluppata, anche muovendo dalla constatazione degli scarsi risultati prodotti su questo piano dalla Direttiva *Open Data*: «talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, *spesso non sono messe a disposizione*, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, *nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile*»[27].

Il Regolamento perciò mira, nella sua parte dedicata al settore pubblico, a sbloccare quelle particolari categorie di dati soggetti a regimi speciali che ne impedivano la riutilizzazione[28], incoraggiando l'adozione di tecniche di anonimizzazione, aggregazione *et al.* dei dati protetti in maniera tale da assicurare il pieno rispetto dei diritti di terzi[29].

commerciali o non commerciali conformemente ai capi III e IV. 2. Gli Stati membri provvedono affinché i documenti i cui diritti di proprietà intellettuale sono detenuti da biblioteche, comprese le biblioteche universitarie, musei e archivi, e i documenti in possesso delle imprese pubbliche siano riutilizzabili a fini commerciali o non commerciali, qualora il loro riutilizzo sia autorizzato, conformemente ai capi III e IV».

24. Art. 4 (*Trattamento delle richieste di riutilizzo)*: «1. Gli enti pubblici esaminano le richieste di riutilizzo e mettono i documenti a disposizione del richiedente, ove possibile e opportuno per via elettronica o, se è necessaria una licenza, mettono a punto l'offerta di licenza per il richiedente entro un lasso di tempo ragionevole e coerente con quello previsto per l'esame delle richieste di accesso ai documenti».
25. Art. 6 (*Principi di tariffazione)*: «1. Il riutilizzo di documenti è gratuito. Tuttavia, può essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato. 2. In via eccezionale il paragrafo 1 non si applica: a) a enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico; b) a biblioteche, comprese le biblioteche universitarie, musei e archivi; c) alle imprese pubbliche […]».
26. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 ("Regolamento sulla governance dei dati").
27. Considerando n. 6, nostro il corsivo, ove si ribadisce che «l'idea che i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società è da tempo parte integrante delle politiche dell'Unione. La direttiva (UE) 2019/1024 e la normativa settoriale dell'Unione garantiscono che gli enti pubblici rendano facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che producono».
28. *Ivi*: «A causa della sensibilità di tali dati, prima che essi siano messi a disposizione si devono soddisfare alcuni requisiti procedurali tecnici e giuridici al fine, se non altro, di garantire il rispetto dei diritti di terzi sui dati in questione o di limitare l'effetto negativo sui diritti fondamentali, sul principio di non discriminazione e sulla protezione dei dati. L'adempimento di tali requisiti risulta abitualmente molto dispendioso in termini di tempo e richiede un livello molto elevato di conoscenze. Ciò ha determinato un utilizzo insufficiente di tali dati. Per quanto alcuni Stati membri stiano istituendo strutture, procedure o adottando norme per agevolare tale tipo di riutilizzo, ciò non accade in tutta l'Unione. Al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, sono necessarie condizioni chiare per l'accesso a tali dati e il loro utilizzo in tutta l'Unione».
29. Considerando n. 7: «Esistono tecniche che consentono l'analisi di banche dati contenenti dati personali, quali l'anonimizzazione, la privacy differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici o metodi analoghi, nonché altri metodi all'avanguardia di tutela della vita privata che potrebbero contribuire a

Il *Data Governance Act*, come accennato, fornisce per la prima volta alcune importanti definizioni, relative ai concetti di "dato"[30], di "riutilizzo" del dato pubblico[31], di "titolare dei dati"[32], di "utente dei dati"[33] e di "condivisione dei dati"[34].

Per quanto concerne il profilo pubblicistico, il Regolamento disciplina (art. 5) le condizioni per il riutilizzo di una o più delle categorie di dati protetti *ex* art. 3, par. 1[35], detenute da enti pubblici, prescrivendo che esse siano pubbliche, non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo. In ogni caso, tali condizioni non debbono «limitare la concorrenza»[36]. Il Regolamento prevede (art. 6) che gli enti pubblici che consentono il riutilizzo delle categorie di dati protetti di cui sopra possano imporre tariffe non discriminatorie, proporzionate, oggettivamente giustificate (in particolare, per l'eventuale trattamento applicato al fine di garantire i diritti dei terzi; *e.g.,* anonimizzazione, aggregazione etc.) e che non limitino il gioco concorrenziale. La gestione è

un trattamento dei dati maggiormente rispettoso della vita privata. Gli Stati membri dovrebbero fornire sostegno agli enti pubblici affinché utilizzino in maniera ottimale tali tecniche, rendendo così disponibili quanti più dati possibili per la condivisione. L'applicazione di tali tecniche, unite a valutazioni d'impatto globali in materia di protezione dei dati e ad altre tutele può contribuire a una maggiore sicurezza nell'utilizzo e riutilizzo dei dati personali e dovrebbe garantire il riutilizzo sicuro dei dati commerciali riservati a fini statistici, di ricerca e di innovazione. […]».

30. Art. 2, par. 1, n. 1): «"dati": qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».
31. Art. 2, par. 1, n. 2): «"riutilizzo": l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico».
32. Art. 2, par. 1, n. 8): «"titolare dei dati": una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli».
33. Art. 2, par. 1, n. 9): «"utente dei dati": una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali».
34. Art. 2, par. 1, n. 10): «"condivisione dei dati": la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».
35. Ai sensi dell'art. 3, par. 1, si tratta dei dati protetti per: a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; o d) protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024.
36. Ai sensi del par. 3 dell'art. 5, «Gli enti pubblici garantiscono, conformemente al diritto dell'Unione e nazionale, la tutela della natura protetta dei dati. Essi garantiscono il rispetto dei requisiti seguenti: a) concedere l'accesso per il riutilizzo dei dati soltanto qualora l'ente pubblico o l'organismo competente abbia garantito, in seguito alla richiesta di riutilizzo, che i dati sono stati: i) anonimizzati, nel caso di dati personali; e ii) modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione, nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale; b) accedere ai dati e riutilizzare gli stessi da remoto all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico; c) accedere ai dati e riutilizzare gli stessi all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro, rispettando rigorose norme di sicurezza, a condizione che l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi».

affidata ad un sistema di sportelli unici (art. 8), con articolazione settoriale, regionale o locale.

Ad ogni modo, è opportuno chiarire che il Regolamento non fissa alcun obbligo per gli enti pubblici di acconsentire al riutilizzo dei dati, ma stabilisce una serie di regole comuni che debbono applicarsi qualora l'ente, sia pure dietro compenso, decida di consentirne l'utilizzo.

L'ente pubblico può inoltre svolgere attività di fornitura di "servizi di intermediazione dei dati", nei termini di cui si dirà *infra*, e rivestire altresì il ruolo di "titolare dei dati" ai sensi del Regolamento, ovvero di quel soggetto a cui l'interessato può richiedere di mettere i propri dati, siano essi personali o non personali, a disposizione di un soggetto terzo, "utente dei dati", che ha diritto di utilizzarli per finalità commerciali o non commerciali[37].

3. La condivisione e l'accesso ai dati del settore privato

Si è detto che la recente regolazione europea mira a liberare enormi quantità di dati a beneficio del mercato e dunque a favorire quanto più possibile la loro circolazione e condivisione nel rispetto dei diritti dei soggetti interessati e dei terzi a vario titolo coinvolti. Con molta più prudenza rispetto a quanto osservato per il settore pubblico, la disciplina di favore per la condivisione e l'accesso ai dati coinvolge anche il settore privato. In particolare, come si vedrà in appresso, l'Unione ha varato per lo più norme incentivanti la condivisione volontaria dei dati e solo in rare ed eccezionali occasioni ha previsto formule cogenti di accesso ai dati da parte dei soggetti pubblici o di soggetti terzi del mercato.

3.1. Il profilo privatistico del *Data Governance Act*

Proseguendo la nostra disamina, muoviamo verso il lato privatistico del *Data Governance Act*. In particolare, le fattispecie rilevanti sono quelle dei "servizi di intermediazione dei dati"[38] e dell'"altruismo dei dati"[39].

Con riferimento ai primi, si tratta di attività di intermediazione volta a far instaurare rapporti *commerciali* di condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e utenti dei dati, dall'altro (Capo III del Regolamento).

Diversamente, l'altruismo dei dati mira a favorire la condivisione volontaria di dati *senza compenso* (salvo il rimborso dei costi sostenuti)

37. Ciò può avvenire sia nell'ambito di una "intermediazione dei dati" di cui al Capo III del Regolamento, sia nell'ambito dell'"altruismo dei dati" di cui al Capo IV, di cui si dirà *infra*.

38. Art. 2, par. 1, n. 11): «"servizio di intermediazione dei dati": un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di: a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali».

39. Art. 2, par. 1, n. 16): «"altruismo dei dati": la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

per obiettivi di interesse generale (Capo IV del Regolamento).

In entrambi i casi, il cuore della proposta è la condivisione dei dati secondo la logica della non rivalità e secondo il metodo della volontarietà: il regolamento non introduce, come accennato già per il settore pubblico, alcun obbligo di condivisione[40], ma promuove e regolamenta le forme attraverso le quali tale condivisione può realizzarsi. In particolare, regole stringenti sono fornite in merito alle *Condizioni per la fornitura di servizi di intermediazione dei dati* (art. 12) e ai *Requisiti generali per la registrazione in un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute* (artt. 17 ss.).

L'obiettivo a tendere di questa legislazione di favore per la condivisione è perciò quello della creazione di "spazi comuni europei di dati", di cui si accennava, ossia «quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile»[41].

3.2. Il *Digital Services Act* e il *Digital Markets Act*

Non a una logica di condivisione, ma di "accessibilità", risponde la disciplina prevista nel *Digital Services Act*[42] e nel *Digital Markets Act*[43]. Come noto, i due regolamenti varati dall'Unione nel 2022 hanno come obiettivo la regolazione delle grandi piattaforme digitali, il primo nell'ottica di assicurare responsabilità e trasparenza dei prestatori di servizi di intermediazione online e il secondo nell'ottica di regolamentare *ex ante* il comportamento di mercato delle imprese che forniscono servizi di piattaforma di base, c.d. *gatekeeper*. Senza pretesa alcuna di voler qui sintetizzare la complessa disciplina prevista dai due corposi regolamenti (pienamente applicabili a partire da febbraio e marzo 2024), si può qui osservare – ai nostri fini – quanto segue.

Quel che emerge è un regime tutt'affatto speciale per i dati delle imprese che rientrano nell'ambito soggettivo di applicazione di queste due normative: i dati sono sì *asset* patrimoniali dell'impresa (dunque regolarmente protetti dalle normative in materia di proprietà, *data protection* e segretezza commerciale) ma "accessibili" da un numero chiuso di soggetti che vengono puntualmente indicati.

Per quanto riguarda il DSA, l'art. 40 prevede la possibilità per il Coordinatore dei servizi digitali del luogo di stabilimento o la Commissione di chiedere l'accesso o la comunicazione di dati specifici, compresi i dati relativi ai sistemi algoritmici. Tale richiesta può comprendere, ad esempio, i dati necessari a valutare i rischi e gli eventuali danni derivanti dai sistemi delle *Very Large Online Platforms*, i dati relativi alla precisione, al funzionamento e alle prove dei sistemi algoritmici per la moderazione dei contenuti, dei sistemi di raccomandazione o dei sistemi pubblicitari, compresi, se del caso, i dati

40. Si veda il considerando n. 27: «si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati. I servizi di intermediazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato, prevedendo nel contempo un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati. […]».

41. *Ibidem*.

42. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

43. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828.

di addestramento e gli algoritmi, oppure i dati sui processi e i risultati dei sistemi di moderazione dei contenuti o dei sistemi interni di gestione dei reclami. L'accesso ai dati è altresì riconosciuto ai ricercatori abilitati[44] allo scopo di condurre ricerche che contribuiscano al rilevamento, all'individuazione e alla comprensione dei rischi sistemici nell'Unione[45] e per la valutazione dell'adeguatezza, dell'efficienza e degli impatti delle misure di attenuazione dei rischi[46].

Per quanto riguarda invece il DMA, l'accesso ai dati detenuti dai *gatekeeper* non è solamente garantito – senza particolari limitazioni – alla Commissione nell'ambito dei poteri di indagine di cui all'art. 21 del Regolamento[47], ma è altresì assicurato agli "utenti commerciali"[48]. In particolare, ai sensi dell'art. 6, par. 10, il *gatekeeper* è tenuto a fornire a titolo gratuito agli utenti commerciali e a terzi autorizzati da un utente commerciale, su richiesta, «un accesso efficace, di elevata qualità, continuo e in tempo reale a dati aggregati e non aggregati, compresi i dati personali», garantendo alle stesse condizioni «l'uso di tali dati, che sono forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base […] da parte di tali utenti commerciali e degli utenti finali che si avvalgono di prodotti o servizi forniti da tali utenti commerciali».

Non solo, sempre ai sensi dell'art. 6, ma par. 11, alcuni dei dati in possesso dei *gatekeeper* ricevono una disciplina sostanzialmente equiparabile a quella di una *essential facility*[49], prevedendosi che il gatekeeper garantisca alle imprese terze che forniscono motori di ricerca online, su loro richiesta, «l'accesso a condizioni eque, ragionevoli e non discriminatorie a dati relativi a posizionamento, ricerca, click e visualizzazione per quanto concerne le ricerche gratuite e a pagamento generate dagli utenti finali sui suoi motori di ricerca online»[50].

3.3. L'*AI Act*

Similmente, anche la proposta di *AI Act*[51] (nella versione aggiornata agli emendamenti proposti dal Parlamento europeo del giugno 2023) fa riferimento alle opportunità generate dalla condivisione dei dati per la formazione, la convalida e la sperimentazione di sistemi di intelligenza artificiale[52].

44. Ai sensi del par. 8 dell'art. 40.
45. Come stabilito a norma dell'articolo 34, paragrafo 1.
46. A norma dell'articolo 35.
47. Cfr. il considerando n. 81, a mente del quale: «È opportuno conferire alla Commissione il potere di richiedere le informazioni necessarie ai fini del presente regolamento. La Commissione dovrebbe in particolare avere accesso a tutti i pertinenti documenti, dati, banche dati, algoritmi e informazioni necessari per avviare e svolgere indagini e per monitorare l'osservanza degli obblighi sanciti dal presente regolamento, a prescindere da chi sia in possesso di tali informazioni, e indipendentemente dalla loro forma o formato, dal supporto su cui sono conservati o dal luogo in cui sono conservati».
48. Ai sensi dell'art. 2, par. 1, n. 21), è utente commerciale «qualsiasi persona fisica o giuridica che, nell'ambito delle proprie attività commerciali o professionali, utilizza i servizi di piattaforma di base ai fini della fornitura di beni o servizi agli utenti finali o nello svolgimento di tale attività».
49. Cfr. *ex multis*, Graef 2016.
50. Non troppo dissimile dall'obbligo di garantire l'accesso ai dati di cui all'art. 6, parr. 10 e 11, è l'obbligo di fornitura di "informazioni" sugli annunci pubblicitari di cui all'art. 5, parr. 9 e 10.
51. Al momento in cui si scrive non è ancora noto il testo definitivo sul quale il 9 dicembre 2023 è stato raggiunto l'accordo politico tra Parlamento e Consiglio e che sarà oggetto di adozione formale da parte dei due organi.
52. Cfr. il considerando n. 45 della versione sopra citata della proposta: «per lo sviluppo e la valutazione dei sistemi di intelligenza artificiale ad alto rischio, è opportuno che alcuni soggetti, come i fornitori, gli organismi notificati e altre entità pertinenti, come i poli di innovazione digitale, le strutture di sperimentazione e i ricercatori, possano accedere e utilizzare serie di dati di alta qualità nell'ambito dei rispettivi settori di attività connessi al presente regolamento. Gli spazi comuni di dati europei istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra le imprese e con le amministrazioni pubbliche nell'interesse pubblico saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di alta qualità per la formazione,

Il Regolamento, la cui versione finale – si ribadisce – non è ancora nota, prevede altresì meccanismi eccezionali di accesso, per così dire "invertito" (cioè da pubblico a privato), funzionali ad assicurare la vigilanza sul rispetto della normativa in materia di sistemi di intelligenza artificiale ad alto rischio: l'autorità nazionale di vigilanza potrà accedere, previa richiesta motivata sotto il profilo della necessarietà, «agli insiemi di dati relativi alla formazione, alla convalida e ai test utilizzati dal fornitore o, se del caso, dall'implementatore» (art. 64 della Proposta).

3.4. Il *Data Act*

Il *Data Act* rappresenta senz'altro il testo normativo più avanzato sul tema dell'accesso e della condivisione dei dati[53]. Il Regolamento persegue diverse finalità d'interesse per quanto qui ci occupa, muovendo dall'idea di rimuovere quanto più possibile gli ostacoli all'accesso e alla condivisione dei dati tra consumatori e imprese, tra imprese, e – a certe condizioni – tra imprese e settore pubblico[54]. Innanzitutto, il Regolamento garantisce che gli utenti[55] di un prodotto connesso[56] o di un servizio correlato[57] (solitamente chiamati "IoT", *Internet of Things*[58]) possano accedere tempestivamente ai

la convalida e la sperimentazione dei sistemi di IA. Ad esempio, nel settore sanitario, lo spazio europeo dei dati sanitari faciliterà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di intelligenza artificiale su tali insiemi di dati, in modo rispettoso della privacy, sicuro, tempestivo, trasparente e affidabile, e con un'adeguata governance istituzionale. Le autorità competenti, comprese quelle settoriali, che forniscono o supportano l'accesso ai dati possono anche sostenere la fornitura di dati di alta qualità per l'addestramento, la convalida e il test dei sistemi di intelligenza artificiale».

53. Si fa riferimento al testo approvato formalmente dal Parlamento Europeo il 9 novembre 2023 e dal Consiglio il 27 novembre 2023, che è in attesa di pubblicazione sulla Gazzetta Ufficiale dell'Unione europea.
54. V. considerando n. 2: «Gli ostacoli alla condivisione dei dati impediscono un'allocazione ottimale dei dati a vantaggio della società. Tali ostacoli comprendono la mancanza di incentivi per i titolari dei dati a stipulare volontariamente accordi di condivisione dei dati, l'incertezza sui diritti e gli obblighi in relazione ai dati, i costi per la conclusione di contratti e l'implementazione di interfacce tecniche, l'elevato livello di frammentazione delle informazioni in silos di dati, la cattiva gestione dei metadati, l'assenza di norme per l'interoperabilità semantica e tecnica, le strozzature che impediscono l'accesso ai dati, la mancanza di prassi comuni di condivisione dei dati e l'abuso degli squilibri contrattuali per quanto riguarda l'accesso ai dati e il loro uso».
55. Ai sensi dell'art. 2, par. 1, n. 12) è definito "utente": «una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato».
56. Ai sensi dell'art. 2, par. 1, n. 5) è definito "prodotto connesso": «un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente».
57. Ai sensi dell'art. 2, par. 1, n. 6) è definito "servizio correlato": «un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso».
58. L'espressione *Internet of Things* si ritiene sia stata formulata per la prima volta nel 1999, con riferimento ai dispositivi RFId (*Radio Frequency Identification*), dall'ingegnere inglese Kevin Ahston, cofondatore dell'Auto-ID Center di Massachussetts; cfr. Ashton 2009. L'IoT si declina pressoché in ogni settore dell'economia: si parla oggi di *smart agriculture* (consistente nel monitoraggio di parametri micro-climatici a supporto dell'agricoltura al fine di migliorare la qualità dei prodotti, ridurre le risorse utilizzate e l'impatto ambientale), di *smart cars* (ovvero la connessione delle auto per comunicare informazioni in tempo reale al consumatore, connessione tra veicoli o tra questi e l'infrastruttura circostante per la prevenzione e la rivelazione degli incidenti), *smart cities* (cioè l'attività di monitoraggio e gestione dei servizi pubblici di una città, come il trasporto pubblico, l'igiene

dati generati dall'uso di tale prodotto[59] o servizio[60] e che possano utilizzare tali dati. Agli utenti è riconosciuto il "diritto" (art. 5)[61] di condividerli con terzi di loro scelta, con conseguente obbligo per i titolari dei dati[62] di metterli a disposizione.

Il Regolamento garantisce inoltre che i titolari dei dati mettano i dati a disposizione dei destinatari dei dati[63] nell'Unione a condizioni eque, ragionevoli e non discriminatorie e in modo trasparente (art. 8), prevedendo pertanto specifiche norme di diritto contrattuale volte a impedire lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo (artt. 13 ss.).

Infine, una delle disposizioni più interessanti e significative è quella che assicura un flusso coattivo di dati dal settore privato al settore pubblico (B2G), in caso di necessità eccezionali[64]. Ai sensi dell'art. 14, infatti, i titolari dei dati sono tenuti a mettere a disposizione degli enti pubblici, della Commissione, della Banca centrale europea o degli organismi dell'Unione, ove vi sia una necessità eccezionale, i dati necessari per lo svolgimento di uno specifico compito di pubblico interesse. Tale forma di "espropriazione" di dati è circondata da molte cautele (art. 15)[65], ma rappresenta senz'altro il primo punto di rottura di quel muro eretto a difesa dei

urbana, l'illuminazione pubblica, e dell'ambiente circostante per migliorarne vivibilità, sostenibilità e competitività), di *smart home* (cioè di soluzioni per la gestione in automatico e/o da remoto degli impianti e degli oggetti connessi dell'abitazione, al fine di ridurre i consumi energetici e migliorare il comfort, la sicurezza dell'abitazione e delle persone), di *smart metering* (cioè di contatori connessi per la misurazione dei consumi di elettricità, gas, acqua, calore, e per la loro corretta fatturazione e telegestione), e di *smart factory* (cioè la connessione dei macchinari, degli operatori e dei prodotti per attivare nuove logiche di gestione della produzione); cfr. Osservatorio Big Data Analytics & Business Intelligence del Politecnico di Milano.

59. Ai sensi dell'art. 2, par. 1, n. 15) sono "dati del prodotto": «dati generati dall'uso di un prodotto connesso e progettati dal fabbricante in modo tale che un utente, un titolare dei dati o un terzo, compreso se del caso il fabbricante, possano reperirli tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo».
60. Ai sensi dell'art. 2, par. 1, n. 16) sono "dati di un servizio correlato": «dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore».
61. Ai sensi dell'art. 5, par. 1: «su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati prontamente disponibili, nonché i pertinenti metadati necessari a interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo continuo e in tempo reale».
62. Ai sensi dell'art. 2, par. 1, n. 12) è definito "titolare dei dati": «una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato».
63. Ai sensi dell'art. 2, par. 1, n. 13) è definito "destinatario dei dati": «una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione».
64. Norma che trova un suo precedente nell'art. 19 da legge francese *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique* che ha introdotto l'art. 3-*bis* della *Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques*, a norma del quale è consentito al settore pubblico di accedere a determinati dati del settore privato per finalità di rilevazioni statistiche obbligatorie.
65. Articolo 15 (*Necessità eccezionale di utilizzare i dati*): «1. Una necessità eccezionale di utilizzare determinati dati ai sensi del presente capo è limitata nel tempo e nella portata e si considera esistente esclusivamente in una

dataset delle grandi piattaforme digitali, spesso proprio grazie alla normativa in materia di *data protection*, e che costituisce tutt'oggi la principale barriera all'ingresso nei mercati digitali (in questo senso, le recenti vicende in materia di divieto di *web scraping* altro non fanno che consolidare il dominio esclusivo delle Big Tech sui dati generati dagli utenti[66]).

3.5. La Proposta di *Financial Data Access Act*

La medesima logica di accessibilità e condivisione dei dati si affaccia, naturalmente, anche nel settore finanziario, nel quale la Commissione europea ha avanzato una proposta di regolamento che mira a disciplinare l'accesso ai dati dei clienti e il relativo utilizzo. L'accesso ai dati finanziari si riferisce all'accesso ai dati e al loro trattamento sia da parte del cliente verso l'impresa, sia – ed è il profilo più delicato – tra imprese.

La proposta muove dalla considerazione per cui «l'*economia dei dati finanziari* dell'Unione» è frammentata, caratterizzata da «*disomogeneità nella condivisione dei dati*, ostacoli e una forte riluttanza dei portatori di interessi a condividere dati al di là dei conti di pagamento». Per conseguenza «*i clienti non beneficiano di prodotti e servizi personalizzati* basati sui dati in grado di soddisfare le loro esigenze specifiche». L'assenza di prodotti finanziari personalizzati «*limita le possibilità di innovazione*, offrendo una scelta più ampia e maggiori prodotti e servizi finanziari ai consumatori interessati che potrebbero altrimenti beneficiare di *strumenti basati sui dati* che li aiutino a compiere scelte informate, a confrontare facilmente le offerte e a passare a prodotti più vantaggiosi che *corrispondano alle loro preferenze sulla base dei loro dati*»[67].

La proposta abbraccia la quasi totalità dei dati dei clienti raccolti o prodotti da enti finanziari[68] nell'ambito dei servizi finanziari[69], ivi incluso il delicatissimo profilo della valutazione del merito di credito, e prevede una serie di

delle circostanze seguenti: a) se i dati richiesti sono necessari per rispondere a un'emergenza pubblica e l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione non può ottenere tali dati con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti; b) in circostanze non contemplate dalla lettera a) e solo nella misura in cui si tratti di dati non personali qualora: i) un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione agisca sulla base del diritto dell'Unione o nazionale e abbia individuato dati specifici la cui mancanza gli impedisce di svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge, quali la redazione di statistiche ufficiali, la mitigazione o la ripresa dopo un'emergenza pubblica; e ii) l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione abbia esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati, compresi, l'acquisto dei dati sul mercato ai prezzi di mercato o il ricorso a obblighi vigenti in materia di messa a disposizione dei dati oppure l'adozione di nuove misure legislative che potrebbero garantire la tempestiva disponibilità dei dati. 2. Il paragrafo 1, lettera b), non si applica alle microimprese e alle piccole imprese. 3. L'obbligo di dimostrare che l'ente pubblico non ha potuto ottenere i dati non personali acquistandoli sul mercato non si applica quando il compito specifico svolto nell'interesse pubblico è la produzione di statistiche ufficiali e quando l'acquisto di tali dati non è autorizzato dal diritto nazionale».

66. Si veda in particolare l'avvio dell'Indagine conoscitiva sul *web scraping* per l'addestramento degli algoritmi di intelligenza artificiale da parte del Garante. Cfr. anche Garante per la protezione dei dati personali, Provvedimento del 17 maggio 2023, n. 201.
67. Considerando n. 6.
68. Ai sensi dell'art. 2, par. 2, della proposta sono "enti finanziari": «a) enti creditizi; b) istituti di pagamento […]; c) istituti di moneta elettronica […]; d) imprese di investimento; e) prestatori di servizi per le cripto-attività; f) emittenti di token collegati ad attività; g) gestori di fondi di investimento alternativi; h) società di gestione di organismi d'investimento collettivo in valori mobiliari; i)imprese di assicurazione e di riassicurazione; j) intermediari assicurativi e intermediari assicurativi a titolo accessorio; k) enti pensionistici aziendali o professionali; l) agenzie di rating del credito; m) fornitori di servizi di crowdfunding; n) fornitori di PEPP; o) prestatori di servizi di informazione finanziaria».
69. Ai sensi dell'art. 2, par. 1, della proposta, i dati dei clienti soggetti all'applicazione del regolamento fanno riferimento a: «a) contratti di credito ipotecario, prestiti e conti […]; b) risparmi, investimenti in strumenti finanziari,

diritti e obblighi in capo a "titolari dei dati"[70] e "utenti dei dati"[71].

In particolare, per quanto qui interessa, l'art. 5 della proposta disciplina l'obbligo per il titolare dei dati di mettere i dati del cliente a disposizione di un terzo (definito, con una formula non felicissima, utente dei dati) a cui lo stesso cliente ha concesso l'autorizzazione all'accesso ai propri dati. Tale messa a disposizione deve avvenire «senza indebito ritardo, in maniera continuativa e in tempo reale».

In sostanza, un *promoter* finanziario che ottenga da una persona, fisica o giuridica, l'autorizzazione ad accedere, ad esempio, ai dati bancari, potrà presentarsi presso la sua banca e ottenere – in qualità di utente dei dati – tutte le informazioni utili a strutturare un prodotto finanziario personalizzato da sottoporgli. I rischi derivanti da potenziali pratiche ingannevoli o aggressive sono arginati da alcune misure (la cui efficacia sarà certamente da verificare) previste dalla normativa: innanzitutto la predisposizione di un "pannello di gestione delle autorizzazioni" a disposizione del cliente nel quale siano elencate tutte le autorizzazioni in essere (art. 8), e poi la configurazione di "sistemi di condivisione di dati finanziari" notificati e vigilati da un'autorità indipendente (artt. 9 ss.).

4. I dati come beni non rivali nella teoria dei beni comuni

La rassegna normativa sin qui svolta mostra abbastanza chiaramente che i dati, personali e non personali, sono destinati ad una sempre maggiore circolazione e che la legislazione europea non rallenta affatto, anzi incoraggia fortemente, questo fenomeno. Non solo. Il processo di allontanamento dal modello proprietario di controllo sui dati (se non di vero e proprio abbandono), di cui si diceva in apertura, conduce a trattare sempre più i dati come "risorse comuni", condivise tra più soggetti. Sullo stesso set di dati potranno coesistere numerose situazioni giuridiche soggettive diverse, ciascuna delle quali foriera di specifici diritti, obblighi, oneri.

La domanda che dunque occorre porsi è: "di chi saranno i dati?". Di coloro ai quali si riferiscono? Di chi li riceve? Di chi li acquista? Di chi li usa? Di chi sa ricavare da essi un valore? Il quesito non è di ordine meramente teorico, ma anzi – come si dirà tra un attimo – dalla risposta a questa domanda possono derivare conseguenze significative sul piano giuridico.

La natura "non rivale" dei dati (questa, sì, certa) potrebbe consentire di rispondere che tutti questi soggetti potranno contemporaneamente vantare un autonomo, non parziario, titolo giuridico sugli stessi dati. Senza indulgere eccessivamente in questioni su cui si è già espressa attenta dottrina[72], può osservarsi come il "valore" che sino ad oggi abbiamo riconosciuto ai dati (principalmente quali corrispettivo di servizi) è destinato ad accrescersi proprio grazie alle successive possibilità di sfruttamento, derivanti dalla condivisione e dall'accesso di terze parti. Con la conseguenza che non soltanto la governance dei dati si caratterizzerà per una dimensione sempre più collettiva[73], ma la natura stessa dei dati è destinata a cambiare: da oggetti di diritti esclusivi a oggetti di diritti collettivi.

Del resto, per quanto recenti accadimenti abbiano confermato che i dati sono *funzionalmente*

prodotti di investimento assicurativi, cripto-attività, beni immobili e altre attività finanziarie correlate, nonché i benefici economici derivanti da tali attività […]; c) diritti pensionistici negli schemi pensionistici aziendali o professionali […]; d) diritti pensionistici sulla fornitura di prodotti pensionistici individuali paneuropei […]; e) prodotti di assicurazione non vita […]; f) dati che fanno parte di una valutazione del merito creditizio di un'impresa, raccolti nell'ambito di una procedura di richiesta di prestito o di una richiesta di rating del credito».

70. Ai sensi dell'art. 3, par. 1, n. 5), il "titolare dei dati" è definito come: «un ente finanziario diverso da un prestatore di servizi di informazione sui conti che raccoglie, conserva e altrimenti tratta i dati di cui all'articolo 2, paragrafo 1».

71. Ai sensi dell'art. 3, par. 1, n. 6), l'"utente dei dati" è definito come: «una delle entità di cui all'articolo 2, paragrafo 2, che, previa autorizzazione di un cliente, ha accesso legittimo ai dati del cliente di cui all'articolo 2, paragrafo 1».

72. Versaci 2022, p. 13 ss., laddove evidenzia le incongruenze dell'applicazione di un paradigma strettamente proprietario al regime giuridico dei dati, in particolare non personali.

73. Resta 2022, p. 971 ss.; cfr. anche Iannuzzi 2021, p. 31 ss.; Bravo 2021, p. 199 ss.

utilizzati al posto del denaro (sia dalle grandi piattaforme che dai singoli utenti)[74], i dati non sono – *strutturalmente* – beni comparabili al denaro. Il fenomeno di *impoverimento-arricchimento* che si verifica in una transazione basata su valori monetari, non si realizza laddove la controprestazione di una obbligazione sia costituita da dati: il consumatore "paga", ma non si impoverisce. I dati che lo riguardano continuano ad essere *anche* suoi.

Queste forme di "compossesso"[75], dunque, unite alle proporzioni di larga scala assunte dai *big data* collazionati dai grandi *player* economici globali, inducono a considerare seriamente una loro qualificazione alla stregua di "beni comuni" (*commons*)[76].

Sebbene non esista un univoco concetto giuridico di beni comuni[77], questa categorizzazione può risultare utile non solo al fine di definire lo statuto giuridico dei dati all'indomani di questa imponente ondata regolatoria europea, ma altresì a giustificare le sempre maggiori istanze di accesso e condivisione dei dati, specie nel flusso che va dal settore privato a quello pubblico.

Andiamo con ordine e muoviamo anzitutto dalla prospettiva economica: i beni comuni sono tradizionalmente considerati "rivali" e "non escludibili"[78], ragion per cui si verifica quella che Garret Hardin chiamava la "tragedy of commons": tutti coloro che concorrono allo sfruttamento della risorsa sono anche coloro che ne determinano l'esaurimento[79]. L'unico modo per evitarlo viene così da questi individuato nella proprietà pubblica, che sottrae i beni alla appropriazione individuale. Teorie successive hanno però superato la dicotomia tra privato e pubblico, accedendo a forme intermedie di governo collettivo dei beni comuni. È questa in particolare l'impostazione propria di Elinor Ostrom[80], premio Nobel per l'economia del 2009, la quale ha dimostrato come assetti "istituzionali", non pubblici, nel governo dei beni collettivi siano in grado di assicurare nel tempo la *sostenibilità* dello sfruttamento della risorsa collettiva, di fatto riconoscendo lo spazio per una terza via, tra stato e mercato, tra pubblico e privato[81].

Ebbene, tornando al nostro campo d'indagine, i dati sono la risorsa collettiva globale del nostro tempo (per giunta non rivale, dunque inesauribile), il cui governo è a tutt'oggi in mano a pochi, enormi, poteri privati[82], che esercitano su di essi un controllo di fatto esclusivo ed escludente. I dati, infatti, dal momento in cui sono "rilasciati" dall'interessato al titolare del trattamento, si inseriscono in circuiti economici di larghissima scala a tutto vantaggio delle *Big Tech*, mentre gli utenti si limitano a beneficiare di qualche servizio gratuito.

Considerare quindi i dati (specie quelli personali e quelli che derivano dai dati personali a séguito di procedimenti di anonimizzazione) come "beni comuni"[83] avrebbe il pregio di riconoscere la provenienza *collettiva* e *relazionale* di tale fonte di

74. V. *supra*, nota 3.

75. Che riecheggiano forme di proprietà collettiva antecedenti all'avvento dello stato liberale e del diritto di proprietà come diritto assoluto. Cfr. Grossi 1977, *passim*.

76. Cfr. sul tema Fia 2021, p. 185 ss.

77. Si veda Cerulli Irelli-De Lucia 2014, p. 6 ss., laddove rilevano almeno 4 accezioni diverse: i) interessi e valori generali, di tono costituzionale; ii) beni immateriali di importanza centrale per la società; iii) cose in senso giuridico strumentali all'esercizio di diritti fondamentali della persona; iv) spazi fisici goduti da una collettività. Cfr. anche Marella 2012, p. 18; Hess-Ostrom 2003, p. 114 ss.; in generale sul tema, si veda: Arena 2022, p. 647 ss; Cerulli Irelli 2022, p. 639 ss.; Ciervo 2012; Rodotà 2013, p. 105.

78. Brosio 2021, pp. 32-34.

79. Hardin 1968, p. 162 ss.

80. In particolare, Ostrom 1990.

81. Cfr. anche Ostrom-Schroeder-Wynne 1993.

82. Sia consentito rinviare a Cremona 2023. Cfr. Ferrarese 2022, p. 138. Betzu 2020. O ancora l'intero fascicolo n. 3/2021 della rivista *Diritto Pubblico* dedicato ai poteri privati, del quale si richiamano qui – sul tema Big Tech – i contributi di Betzu 2021; Brandimarte-Pecchi-Piga 2021; Di Gaspare 2021; Ferrarese 2021; Libertini 2021; Pardolesi 2021.

83. Cfr. Nissenbaum 2009; Sanfilippo-Frischmann-Standburg 2018; Wong-Henderson-Ball 2022; Mills 2019.

ricchezza e dunque di giustificare anche politiche "restitutorie", come quella della ridetta "espropriazione" dei dati per necessità eccezionali (*ex* art. 14 del *Data Act*) o dell'accesso pubblico ai dati detenuti dai privati per finalità di beneficio comune.

5. *Data for Good*: prospettive di *data sharing* per le imprese nel quadro della regolamentazione di sostenibilità

Iniziare a considerare – a certi fini e a certe condizioni – i dati in possesso delle imprese (o almeno quelli delle grandi piattaforme digitali) come beni comuni può creare le premesse per interventi normativi che restituiscano agli utenti, sia pure indirettamente, una parte della ricchezza generata proprio a partire dai dati loro riferibili. Le petizioni in questo senso sono molte e crescenti[84].

Non è difficile immaginare l'ampiezza dei settori nei quali i dati in mano a soggetti privati potrebbero risultare utili per il bene comune[85]: si pensi banalmente ai dati sul traffico e in generale sugli spostamenti, con significativi potenziali impatti diretti sull'ambiente, ai dati sull'istruzione, sull'accesso al lavoro, a quelli sulla salute ricavati dagli *wearables*, e a tutte le informazioni che sarebbero preziose nella definizione di politiche pubbliche e nell'erogazione dei servizi pubblici[86].

Secondo recenti rilevazioni, l'accesso degli enti pubblici (in particolare delle amministrazioni locali[87]) ai dati del settore privato di interesse pubblico è ancora una pratica emergente e sporadica[88]. Alcuni report riferiscono di una percepita asimmetria di potere (a vantaggio del settore privato) nella condivisione dei dati verso le amministrazioni locali, non esistendo ad oggi ancora strumenti giuridici vincolanti per l'accesso a tali informazioni. Solo si danno alcune virtuose esperienze volontarie di c.d. *data philantropy*[89].

Vi sono però, anche in una prospettiva *de jure condito*, strumenti giuridici che potrebbero essere valorizzati al fine di promuovere la condivisione *stabile* di dati dal settore privato a quello pubblico. Il riferimento è al *framework* normativo cosiddetto ESG (*environmental*, *social*, *governance*) e in particolare alla Direttiva europea in materia di *Corporate Sustainability Reporting* (c.d. CSRD)[90], entrata

84. Si veda già Mazzuccato 2018, ove afferma: «Let's not forget that a large part of the technology and necessary data was created by all of us, and should thus belong to all of us. The underlying infrastructure that all these companies rely on was created collectively (via the tax dollars that built the internet), and it also feeds off network effects that are produced collectively. There is indeed no reason why the public's data should not be owned by a public repository that sells the data to the tech giants, rather than vice versa. But the key issue here is not just sending a portion of the profits from data back to citizens but also allowing them to shape the digital economy in a way that satisfies public needs. Using big data and AI to improve the services provided by the welfare state – from health care to social housing – is just one example».

85. Alemanno 2018; OECD 2015; Farmer-McCosker-Albury-Aryani 2023.

86. Si vedano in questa direzione le iniziative, ad esempio, del *Data for Road Safety* o dei *Data Collaboratives*. Cfr. Commissione europea 2020.

87. Cfr. Giannelli-Pagnanelli 2023; Vigorito 2023, p. 697 ss.; Hardinges 2019.

88. Micheli 2022. L'articolo riporta i risultati di una ricerca che ha esaminato la condivisione dei dati B2G nelle amministrazioni locali europee. Basandosi su interviste con responsabili di progetto di dodici comuni, lo studio ha contestualizzato l'accesso ai dati del settore privato nella prospettiva di coloro che lavorano nel settore pubblico.

89. McKeever-Greene-MacDonald-Tatian 2018.

90. La CSRD UE 2022/2464 (pubblicata nella Gazzetta Ufficiale UE il 16 dicembre 2022) modifica la normativa europea emendando la Direttiva 2004/109/CE sull'armonizzazione degli obblighi di trasparenza riguardanti le informazioni sugli emittenti i cui valori mobiliari sono ammessi alla negoziazione in un mercato regolamentato; la Direttiva 2006/43/CE relativa alle revisioni legali dei conti annuali e dei conti consolidati; le Direttive 2013/34/UE e 2014/95/UE relative ai bilanci d'esercizio, ai bilanci consolidati, alle relative relazioni di talune tipologie e alla comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni; il Regolamento UE 537/2014 sui requisiti specifici relativi alla revisione legale dei conti di enti di interesse pubblico. Cfr. in tema Genovese 2023, p. 88 ss.; Fortunato 2019, p. 420 ss.

in vigore il 5 gennaio 2023, in forza della quale le imprese ricadenti nell'ambito soggettivo di applicazione della direttiva[91] saranno tenute a comunicare al pubblico "informazioni sulla sostenibilità" che, come è noto, si declina nei fattori ambientali, sociali e di governo dell'impresa. A questa si affianca la Proposta di *Corporate Sustainability Due Diligence Directive* (CSDDD)[92], che, in omaggio a un dichiarato *stakeholderism*, integra i doveri di diligenza dell'impresa nei confronti di tutti i portatori di interesse[93].

Ebbene, se gli obblighi positivi in campo ambientale e di governance sono forse più chiari e normati, quelli in campo sociale sono, a detta dei più, ancora sfuggenti e non chiaramente definiti. Sotto questo profilo, l'adozione di policy di *data sharing* rappresenta per le imprese una opportunità non soltanto per concorrere a finalità di beneficio comune, ma altresì di compliance ad un plesso normativo – quello sulla sostenibilità – sempre più rilevante e penetrante.

Riferimenti bibliografici

A. Alemanno (2018), *Data for good: unlocking privately held data to the benefit of the many*, in "European Journal of Risk Regulation", vol. 9, 2018, n. 2

G. Arena (2022), *Da beni pubblici a beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

K. Ashton (2009), *That 'Internet of Things' Thing*, in "rfidjournal.com", 22 June 2009

V. Bachelet (2023), *La Corte di giustizia sul caso Meta: trattamento di dati e "prezzo" del consenso*, in "Pactum", 2023, n. 4

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

M. Betzu (2020), *Poteri pubblici e poteri privati nel mondo digitale*, in P. Costanzo, P. Magarò, L. Trucco (a cura di), "Il diritto costituzionale e le sfide dell'innovazione tecnologica", 2020

L. Brandimarte, L. Pecchi, G. Piga (2021), *Le imprese Big Tech: schiave delle leggi per poter essere liberi?*, in "Diritto pubblico", 2021, n. 3

F. Bravo (2021), *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in "Contratto e impresa Europa", 2021, n. 1

C. Brescia Morra (2022), *Chi salverà il mondo? Lo stato o le grandi corporations? ESG: una formula ambigua e inutile*, in "Rivista trimestrale di diritto dell'economia", 2022, n. 4

G. Brosio (2021), *Economia pubblica moderna*, Giappichelli, 2021

91. La direttiva riguarda: i) grandi imprese non quotate che alla data della chiusura del bilancio, anche su base consolidata, abbiano superato almeno due dei seguenti criteri dimensionali: 250 numero medio di dipendenti; € 20 milioni di stato patrimoniale; € 40 milioni di ricavi netti; ii) piccole e medie imprese quotate (escluse le micro-imprese). Sono, inoltre, compresi gli istituti di credito di piccole dimensioni non complessi e le imprese di assicurazioni dipendenti da un Gruppo; iii) imprese e figlie di succursali con capogruppo extra-UE per le quali la capogruppo abbia generato in UE ricavi netti superiori a € 150 milioni per ciascuno degli ultimi due esercizi consecutivi e almeno: un'impresa figlia soddisfi i requisiti dimensionali della CSRD; una succursale abbia generato ricavi netti superiori a € 40 milioni nell'esercizio precedente.

92. Commissione europea, Proposta della Commissione di Direttiva del Parlamento europeo e del Consiglio relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la Direttiva (UE) 2019/1937, COM/2022/71, del 23 febbraio 2022. In tema cfr. Racugno-Scano 2022, p. 726 ss.; Ventoruzzo 2021, p. 386 ss.; nonché l'intero fascicolo 1/2022 della rivista *Analisi Giuridica dell'Economia*, con commenti, tra gli altri di Tombari, Strambelli, Rescigno.

93. Tra i commenti più scettici, Brescia Morra 2022, p. 78 ss.

V. Cerulli Irelli (2022), *Proprietà, beni pubblici, beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

V. Cerulli Irelli, L. De Lucia (2014), *Beni comuni e diritti collettivi*, in "Politica del diritto", 2014, n. 1

A. Ciervo (2012), *I beni comuni*, Ediesse, 2012

Commissione europea (2020), *GDPR – A fabric of a success story*, June 2020

Commissione europea (2020), *Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020

Commissione europea (2019), *SME panel consultation - B2B Data Sharing*, October 2019

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

A. Davola (2021), *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in "Diritto di internet", 2021, n. 1

A. De Franceschi, M. Lehmann (2015), *Data As Tradable Commodity and New Measures for Their Protection*, in "The Italian Law Journal", vol. 1, 2015, n. 1

G. De Gregorio, F. Paolucci (2022), *Dati e intelligenza artificiale all'intersezione tra mercato e democrazia*, in E. Cremona, F. Laviola, V. Pagnanelli, "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

G. Di Gaspare (2021), *Poteri privati e Corporation nella globalizzazione*, in "Diritto pubblico", 2021, n. 3

European Data Protection Supervisor (2020), *Opinion 3/2020, Opinion on the European strategy for data*, 16 June 2020

J. Farmer, A. McCosker, K. Albury, A. Aryani (2023), *Data for social good. Non-Profit Sector Data Projects*, Palgrave Macmillan, 2023

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

M.R. Ferrarese (2021), *Privatizzazioni, poteri invisibili e infrastrutture giuridiche globali*, in "Diritto pubblico", 2021, n. 3

T. Fia (2021), *An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons*, in "Global Jurist", 2021

S. Fortunato (2019), *L'informazione non-finanziaria nell'impresa socialmente responsabile*, in "Giurisprudenza commerciale", 2019, n. 3

A. Galiano, A. Leogrande, S.F. Massari, A. Massaro (2020), *I dati non personali: la natura e il valore*, in "Rivista italiana di informatica e diritto", 2020, n. 1

A. Genovese (2023), *L'armonizzazione del reporting di sostenibilità delle imprese azionarie europee dopo la CSRD*, in "Contratto e impresa", 2023

M. Giannelli, V. Pagnanelli (2023), *Smart cities*, Giappichelli, 2023

I. Graef (2016), *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International, 2016

P. Grossi (1977), *Un altro modo di possedere*, Giuffrè, 1977

G. Hardin (1968), *The tragedy of the Commons*, in "Science", 1968

J. Hardinges (2019), *Do cities have access to the private sector data they need to make effective decisions?*, Open Data Institute, 23 July 2019

C. Hess, E. Ostrom (2003), *Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource*, in "Law & Contemporary Problems", 2003

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

M. Libertini (2021), *Sugli strumenti giuridici di controllo del potere economico*, in "Diritto pubblico", 2021, n. 3

M.R. Marella (a cura di) (2012), *Per un diritto dei beni comuni. Oltre il pubblico e il privato*, Ombre Corte, 2012

M. Mazzuccato (2018), *Let's make private data into a public good*, in "MIT Technology Review", 27 June 2018

B. McKeever, S. Greene, G. MacDonald, P. Tatian (2018), *Data Philanthropy. Unlocking the Power of Private Data for Public Good*, in "Urban Institute", 24 July 2018

M. Micheli (2022), *Public bodies' access to private sector data: The perspectives of twelve European local administrations*, in "First Monday", vol. 27, 2022, n. 2

S. Mills (2019), *Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership*, 24 September 2019

H. Nissenbaum (2009), *Privacy in context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009

OECD (2015), *Data-driven innovation: big data for growth and well-being*, 2015

E. Ostrom (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990 (trad.it.: *Governare i beni collettivi*, Marsilio, 2006)

E. Ostrom, L. Schroeder, S. Wynne (1993), *Institutional Incentives and Sustainable Development: Infrastructure Policies in Perspective*, Oxford, Westview Press, 1993

R. Pardolesi (2021), *Piattaforme digitali, poteri privati e concorrenza*, in "Diritto pubblico", 2021, n. 3

R. Pardolesi, R. Van den Bergh, F. Weber (2020), *Facebook e i peccati da «Konditionenmissbrauch»*, in "Mercato, concorrenza e regole", 2020, n. 3

K. Pistor (2019), *The Code of Capital. How the Law Creates Wealth and Inequality*, Princeton University Press, 2019

G. Racugno, D. Scano (2022), *Il dovere di diligenza delle imprese ai fini della sostenibilità: verso un Green Deal europeo*, in "Rivista delle società", 2022, n. 4

G. Resta (2022), *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

S. Rodotà (2013), *Mondo delle persone, mondo dei beni*, in Id., "Il diritto di avere diritti", Laterza, 2013

A. Sandulli (2021), *Il diritto quale infrastruttura per i poteri privati? A proposito di un libro di Katharina Pistor*, in "Diritto Pubblico", 2021, n. 3

M. Sanfilippo, B. Frischmann, K. Standburg (2018), *Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework*, in "Journal of Information Policy", vol. 8, 2018

M. Ventoruzzo (2021), *Note minime sulla responsabilità civile nel progetto di direttiva Due Diligence*, in "Rivista delle società", 2021, n. 2-3

G. Versaci (2022), *Note minime sulla circolazione dei dati nei rapporti tra imprese*, in "Studi e materiali. Rivista semestrale del Consiglio nazionale del notariato", 2022, n. 1

A. Vigorito (2023), *Government Access to Privately-Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models*, in G. Resta, V. Zeno-Zencovich (eds.), "Governance of/through Big Data", RomaTrE-Press, 2023

S.D. Warren, L. Brandeis (1890), *The Right to Privacy*, in "Harvard Law Review", IV (5), 1890

J. Wong, T. Henderson, K. Ball (2022), *Data Protection for the common good: Developing a framework for a data-protection-focused data commons*, in "Data & Policy", 2022, n. 4, e3

H. Zech (2015), *Information as Property*, in "Journal of Intellectual Property, Information Technology and E-Commerce Law", vol. 6, 2015, n. 3

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0125 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Stefano Torregiani

Il *Data Act*: una versione europea del *Data Nationalism*?

La datificazione ha contribuito alla silente e graduale erosione della sovranità dell'Unione europea: dalla miniera d'oro di dati prodotti dai cittadini europei hanno attinto sistematicamente soggetti stranieri, pubblici e privati, dotati di infrastrutture, tecnologie e competenze proprie, mentre gli Stati membri sono per lo più rimasti inerti e il tessuto industriale europeo è rimasto al palo del progresso digitale. Le ultime iniziative intraprese dal legislatore continentale in materia di "diritto dei dati" mirano ad arginare questa progressiva corrosione della autorità dell'Unione attraverso il rafforzamento di una impalcatura ordinamentale dimostratasi fin troppo vulnerabile. Questo contributo si focalizza sull'ultimo di tali provvedimenti normativi: il *Data Act*, ossia il testo regolamentare, di recente approvazione, volto a garantire una migliore allocazione del valore delle informazioni generate o raccolte nel contesto dell'utilizzo di prodotti e servizi appartenenti alle tecnologie dell'informazione e della comunicazione: ci si domanda se il sistema di circolazione dei dati immaginato dal legislatore dell'Unione è inquadrabile nel fenomeno del cd. *Data Nationalism* e se tale provvedimento potrà tradursi in un fruttuoso tentativo di difendere la sovranità europea attualmente in pericolo, se non proprio compromessa.

Regolamento sui dati – Localizzazione dei dati – Sovranità digitale – Diritto dei dati

Data Act: a European version of Data Nationalism?

The Datafication of the society led to the progressive decrease of the EU sovereignty: data produced by European citizens and companies have been systematically exploited by better equipped and skilled foreign players, thus holding European industrial and technological development back. Some of the acts lately enacted in the EU aim to overturn this detrimental situation through the update of the flawed European data law. This paper focuses on the last of the European Regulation concerning data law, i.e. the Data Act, through which EU institutions seek to reallocate the value of data produced or processed by means of information and communication technologies. Notably, it is questionable whether the data flow legislation setup in EU can be deemed as a Data Nationalism policy and whether this act could be a profitable attempt to defend the European sovereignty.

Data Act – Data Nationalism – Digital sovereignty – Data law

L'Autore è assegnista di ricerca presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Introduzione: l'Unione europea alla prova della datificazione

Il processo di datificazione delle realtà, ossia la trasformazione delle interazioni sociali in dati digitali quantificabili[1], ha portato alla configurazione di uno scenario globale in cui le informazioni, specie di carattere digitale, sono divenute una risorsa imprescindibile per la conduzione di qualsiasi attività di interesse sia pubblico sia privato[2]. In tale rinnovato contesto, i tradizionali elementi su cui si è storicamente basato il potere degli Stati sovrani sono stati messi fortemente in crisi dall'entrata in scena di nuovi attori che, tramite il controllo delle tecnologie su cui transitano i dati, hanno progressivamente acquisito la capacità di influenzare profondamente ogni aspetto della società nella quale viviamo.

Dal canto proprio, l'Unione europea ha dimostrato di patire enormemente tale congiuntura storica per una serie di ragioni di ordine tecnico e giuridico.

In primo luogo, la carenza di infrastrutture, di *expertise* e di investimenti paragonabili a quelli degli altri Stati rivali ha reso il vecchio continente un terreno piuttosto sterile per la crescita di operatori economici autoctoni in grado di sviluppare sistemi che possano quantomeno duellare con i vari GAFAM (Google, Apple, Facebook, Amazon, Microsoft) e BATX (Baidu, Alibaba, Tencent, Xiaomi)[3].

Tale "peccato originale" ha inevitabilmente aperto la strada allo sviluppo di una pesante dipendenza dai fornitori esteri, per la maggioranza siti in territorio statunitense, per la fruizione di servizi di natura latamente digitale (intelligenza artificiale, *cloud computing*, tecnologie 5G e similari)[4].

In secondo luogo, la tradizione costituzionale da cui provengono la maggior parte degli Stati membri dell'Unione europea – e da cui lo stesso ordinamento giuridico dell'Unione trae origine – non può che dimostrarsi refrattaria innanzi alla diffusione di un potere, quello delle *big tech*, che, per un verso, è in grado di influenzare la vita dei consociati in misura pari se non superiore a quella di una autorità pubblica democraticamente eletta, ma per un altro, difetta di qualsivoglia legittimazione popolare e non risulta pienamente conforme ai principi dello Stato di diritto[5].

Stanti le carenze sistemiche che affliggono il nostro continente e il rischio di erosione della

1. VanDijck 2014; Martoni 2020.
2. Surblyte 2016.
3. Polito 2021.
4. Già nel 2019 Kalff-Renda 2019, a p. 173, affermavano che: «current figures show that the bulk of Western world data (an estimated 92%) is currently stored in the United States, whereas only 4% is currently stored in Europe».
5. Non essendo infatti sufficienti i deludenti tentativi di vestire le piattaforme digitali di una parvenza di neutralità nei casi di insorgenza di controversie nascenti nel mondo online, come nell'ipotesi del *Facebook Oversight Board*; si veda in proposito Buratti 2022.

sovranità statuale che ne consegue, l'Unione europea ha reagito a tale situazione sfavorevole muovendosi, innanzitutto, verso la protezione dell'asset più prezioso a sua disposizione: i dati generati dai cittadini e dalle imprese nell'Unione europea. A tal fine, oltre al riconoscimento del diritto alla protezione dei dati personali[6], le istituzioni hanno di recente avviato una profonda riforma dell'ordinamento giuridico in materia di dati. In particolare, con la *Strategia europea per i dati* pubblicata nel 2020 la Commissione europea ha programmato le misure politiche e gli investimenti a sostegno dell'economia dei dati che le istituzioni e gli Stati membri avrebbero dovuto attuare nei successivi cinque anni al dichiarato scopo di rafforzare la sovranità dell'Unione[7].

Questo lavoro intende focalizzarsi su uno degli obiettivi prefigurati nella *Strategia*: la recente approvazione del Regolamento (UE) 2023/2854, noto anche con il nome di Data Act[8]. Nello specifico, verranno esaminati quegli elementi presenti nel testo del provvedimento normativo in questione che risultano utili a fornire una possibile risposta alla domanda che ha ispirato il titolo di questo contributo; si cercherà dunque di comprendere se questo (ennesimo) intervento del legislatore europeo si traduce in una chiusura delle frontiere digitali dell'Unione e, soprattutto, se un simile atteggiamento è in grado di garantire il raggiungimento degli obiettivi prefissati nella *Strategia europea per i dati*.

I paragrafi che seguono saranno dedicati, in primo luogo, alla perimetrazione del concetto di sovranità secondo il significato nuovo che esso ha assunto nell'epoca della datificazione. Successivamente, si passerà all'analisi del legame tra detto concetto e la regolazione della circolazione dei dati, prestando particolare attenzione all'atteggiamento di chiusura diffusosi negli ultimi anni negli ordinamenti giuridici di tutto il mondo. Da ultimo, si procederà ad una prima disamina di quei passaggi presenti nel *Data Act* che possono costituire una idonea base di partenza per comprendere l'orientamento politico del legislatore dell'Unione europea.

2. La regolazione della tecnologia: una questione di sovranità digitale

La corretta individuazione del significato che ha assunto il termine "sovranità" nell'attuale epoca digitale rappresenta una operazione tutt'altro che agevole.

La dottrina ha infatti rilevato l'esistenza di una pluralità di significati astrattamente riconducibili alla nozione di sovranità, la cui portata può assumere una accezione diversa a seconda del punto di vista dell'osservatore, sia esso di carattere giuridico, linguistico, politologico oppure sociale[9]. Qualunque sia il modo in cui la si vuole inquadrare, il comune denominatore di questo ventaglio di significati risiede in quel particolare potere riconosciuto a una organizzazione, storicamente di carattere politico, di esercitare la propria autorità all'interno di un territorio circoscritto, senza subire interferenze provenienti dall'esterno[10].

Adottando una prospettiva costituzionalistica, la sovranità costituisce l'elemento saliente del potere della autorità pubblica che, quantomeno a

6. Per la ricostruzione del percorso storico che ha portato al riconoscimento di tale diritto, si veda Gonzalez Fuster 2014.
7. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati", COM(2020) 66. In particolare, a pag. 6 la Commissione sottolinea che: «Il funzionamento dello spazio europeo di dati dipenderà dalla capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione, come pure nelle competenze digitali, ad esempio l'alfabetizzazione ai dati (data literacy). Ciò contribuirà a sua volta a rafforzare la sovranità tecnologica dell'Europa per quanto riguarda le tecnologie e le infrastrutture abilitanti fondamentali per l'economia dei dati».
8. L'iter per l'entrata in vigore del provvedimento, iniziato il 23 febbraio 2022 con la pubblicazione della "Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo", denominato *Data Act*, è di recente giunto al termine giacché, dopo la sottoscrizione finale avvenuta in data 13 dicembre 2023, il provvedimento è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il 22 dicembre 2023.
9. Per un approfondimento, si veda Couture-Toupin 2019.
10. Pohle-Thiel 2020.

partire dal XVIII secolo, trova nel diritto tanto il suo fondamento, quanto la sua limitazione[11]. Se nella dimensione reale il potere sovrano da limitare era sempre stato quello riconosciuto al monarca o allo Stato-Ente, l'avvento della rivoluzione cibernetica ha sconvolto tale ordine[12], in quanto, introducendo una nuova dimensione nella nostra esistenza, quella virtuale, che si affianca e che impatta pesantemente su quella reale, ha ammesso nella corsa verso la sovranità attori nuovi, che mai prima d'ora avevano potuto vantare un potere equiparabile a quello di uno Stato sovrano.

In tale prospettiva, il processo di datificazione della realtà ha inesorabilmente spinto verso una riconsiderazione della definizione del concetto di "sovranità", non solo per quanto concerne la natura dei soggetti che possono effettivamente qualificarsi come titolari di sovranità, ma soprattutto per quanto riguarda le modalità attraverso le quali la sovranità stessa può essere esercitata. La questione non può più ridursi esclusivamente all'analisi del profilo soggettivo del detentore del potere (sovrano assoluto, entità statuale, popolo e così via), poiché oggi, forse come mai prima nella storia, assume una valenza tanto nuova quanto determinante il mezzo tecnico di cui il sovrano si avvale per acquisire e utilizzare il suo potere.

I commentatori più avveduti hanno individuato la caratteristica distintiva della sovranità dell'era digitale nel potere di calcolo e di automazione garantito dalla moderna tecnologia che, permettendo di prescindere in parte dall'azione umana, rende difficilmente controllabile e giustiziabile l'esercizio della autorità sovrana utilizzando i tradizionali canoni della normazione giuridica e del controllo pubblico[13].

La conseguenza inevitabile di tale cambio di paradigma, che segna altresì la differenza fondamentale tra sovranità e sovranità digitale, coincide con il notevole decremento di rilevanza dell'elemento della territorialità. Se prima il concetto rispecchiava il potere che l'organizzazione era in grado di esercitare su una territorialità definita e sui soggetti che su tale territorio transitavano[14], con l'avvento della rete Internet, caratterizzata per l'appunto dalla cosiddetta "a-territorialità"[15], la partita della sovranità non si gioca più solamente sul piano fisico-spaziale, ma anche su quello virtuale[16].

Ed è proprio su tale piano che le tradizionali entità statali, specie europee, fanno fatica ad imporsi: la sovranità nell'era digitale non può più prescindere dal mezzo tecnico[17], proprio perché attraverso di esso – e, come si vedrà, attraverso i dati che ne costituiscono la linfa vitale[18] – il potere sovrano viene esercitato: se una parte consistente della vita dei singoli si svolge in un ambiente cui è possibile accedere solamente tramite una infrastruttura – che dunque funge da portale interposto tra il reale e il virtuale – il controllo e la gestione

11. Simoncini 2017.
12. Simoncini 2019.
13. Simoncini 2017.
14. Pohle-Thiel 2020.
15. Gardini 2021, spec. pp. 296-301. Ma si veda sul punto Zeno-Zencovich 2016, spec. pp. 14-15, secondo cui l'idea della a-territorialità di Internet è stata oggi superata dalla progressiva espansione dell'intervento statale nella regolazione delle reti.
16. Eloquenti in proposito le parole rilasciate nel 2020 dall'allora presidente del Garante per la protezione dei dati personali italiano, Antonello Soro, il quale ha affermato che: «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, di fronte a sempre nuove spinte illiberali. Sono significativi, in tal senso, i rischi cui un uso manipolativo dei dati personali, anche da parte di potenze estere, può avere sulla sovranità nazionale e sulle scelte politiche essenziali che ne determinano l'esercizio», intervista ad Antonello Soro, aprile 2020, in sito GPDP (doc-web 9317569).
17. Come è stato correttamente puntualizzato da Simoncini 2017: «La sovranità, infatti, oggi non ha più caratteri necessariamente privati o pubblici, personali o collettivi, ma essenzialmente tecnici».
18. Polatin-Reuben-Wright 2014 si riferiscono direttamente al sintagma "data sovereignty" definendolo «the attempt by nation-states to subject data flows to national jurisdictions».

di quella infrastruttura porta con sé l'automatica acquisizione di una autorità sostanzialmente parificabile al potere sovrano che uno Stato vanta sul proprio territorio[19].

Questa svolta epocale ha pesantemente scosso le fondamenta delle democrazie occidentali, le quali si sono trovate costrette a concorrere non più solamente con altre entità pubbliche statuali – come avveniva nell'epoca della sovranità "pre-digitale" – ma con soggetti di natura privata che, proprio grazie al controllo degli strumenti tecnologici, possono esercitare una influenza su un determinato territorio senza neanche la necessità di entrarvi[20].

Dalla presa di coscienza di questa nuova situazione di fatto nascono le più recenti iniziative europee di "regolazione della tecnologia", le quali, benché in linea con quanto avvenuto a partire dagli anni Novanta con la diffusione di Internet[21], si sono moltiplicate negli anni più recenti. Non a caso una delle prime volte in cui il termine trova spazio nelle dichiarazioni ufficiali di esponenti dei governi degli Stati membri coincide con la presentazione dell'iniziativa di Germania e Francia finalizzata alla realizzazione di una infrastruttura digitale di matrice europea, il celebre progetto GAIA-X[22]. Essendo lo scopo quello di predisporre un'alternativa alle big tech estere per la conservazione dei dati dei cittadini e delle imprese europee[23], appare evidente come la realizzazione di siffatto progetto abbia plasmato pesantemente la nozione di sovranità digitale che ha ispirato le azioni delle istituzioni europee[24].

3. Il *Data Nationalism* e la tutela della sovranità

Di fronte all'ingresso delle società private nella contesa verso quella sovranità che prima spettava solo agli Stati, molte entità pubbliche, nazionali o sovranazionali, hanno risposto con l'adozione di numerosi atti normativi, nel tentativo di tamponare il rapido processo di erosione del loro potere. In tale ottica, ognuno dei provvedimenti legislativi aventi ad oggetto la regolazione di una delle svariate dimensioni del mondo della tecnologia digitale vanta infatti una connessione, diretta o indiretta, con il concetto di sovranità. Basti pensare, con riguardo allo scenario europeo, al cosiddetto diritto dei dati (o *data law*)[25], alla proposta di regolazione dell'intelligenza artificiale[26], al *Digital Market Act* o al *Digital Services Act*[27].

19. VanDijck 2020.
20. Cremona 2021.
21. Bertola 2022. Come riconosce l'A., i tentativi di regolazione della rete emersi a cavallo del nuovo millennio si sono caratterizzati più per il modello del "multistakeholderismo", dove governi e teorici della rete libera decidevano di riconoscersi reciproche concessioni in materia di normazione di Internet, piuttosto che per un sistema di regolazione maggiormente prescrittivo tipico della *hard law*.
22. Santaniello 2022.
23. Pagnanelli 2021.
24. È bene notare che il concetto di sovranità varia enormemente a seconda del contesto giuridico e politico di riferimento. In tal senso, la sovranità digitale europea non corrisponderà alla differente declinazione che la nozione di sovranità assume, ad esempio, nella Repubblica popolare cinese, su cui, per un approfondimento si rimanda a Creemers 2020.
25. Con questa espressione si suole fare riferimento a tutte le normative aventi ad oggetto i "dati" generalmente intesi e non solamente a quelle in materia di protezione dei dati personali. Per un approfondimento si veda Streinz 2021.
26. La Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, 21 aprile 2021, COM(2021) 206, più volte modificata, non è ancora entrata in vigore in quanto non risulta ancora concluso l'iter di approvazione.
27. Ci si riferisce, rispettivamente, al Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) e al Regolamento (UE) 2022/2065 del

Fra la vasta gamma di fonti legislative che possono assumere rilievo in tale contesto, il presente lavoro si focalizza sul *data law*: attesa la funzione essenziale e prodromica che la tecnica di trasmissione dei dati ricopre rispetto a tutte le tecnologie digitali oggi disponibili, la regolazione di dette tecnologie deve necessariamente passare attraverso la regolazione della gestione e della circolazione dei dati che le alimentano[28].

Non risulta allora affatto sorprendente che una delle reazioni al fenomeno della datificazione statisticamente più diffuse tra i legislatori di tutti i Paesi del mondo sia stata proprio quella di varare misure normative di *data localization*, consistenti nell'adozione di prescrizioni normative o prassi amministrative che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento oppure che fissano le condizioni per il trasferimento dei dati al di fuori dei confini nazionali[29].

Questa ventata di protezionismo digitale non ha interessato solamente gli Stati membri dell'Unione europea[30], storicamente più sensibile alle questioni di protezione dei dati, specialmente personali, ma ha parimenti riguardato altri Paesi che, intimoriti dall'enorme potere guadagnato dalle *big tech* e dalle nazioni tecnologicamente più avanzate, hanno ritenuto opportuno chiudere le proprie frontiere digitali[31].

È proprio in tale contesto che si avverte in maniera compiuta il passaggio dalla "digital sovereignty" alla "data sovereignty", intesa come «spectrum of approaches adopted by different states to control data generated in or passing through national internet infrastructure»[32], dove tale seconda categoria costituisce un sottoinsieme della prima[33].

Pertanto, l'introduzione di obblighi di localizzazione dei dati viene generalmente interpretata dai legislatori come una delle possibili vie – forse la più percorsa vista l'apparente immediatezza del risultato che è in grado di garantire – per proteggere o riprendere la propria sovranità[34].

Tale ordine di idee ha portato negli ultimi decenni al consolidamento di un fenomeno che è stato dalla dottrina definito come "Data Nationalism"[35]. Detta espressione descrive il novero di politiche che si sono diffuse a partire dalla rivelazione dei programmi di sorveglianza di massa implementati dagli Stati Uniti e che hanno portato all'incremento esponenziale delle misure di localizzazione dei dati[36].

Gli studiosi che si sono occupati delle questioni di *Data Nationalism* e di obblighi di localizzazione non hanno dubbi in merito al fatto che l'attuazione di tali politiche sia più deleteria che vantaggiosa per i singoli governi, giacché la frammentazione di uno spazio ontologicamente interconnesso e senza confini come la rete Internet non farebbe altro che frenare l'innovazione e pregiudicare lo sviluppo delle economie domestiche[37].

Al contempo, non ci si può tuttavia esimere dal constatare che la realtà dei fatti ha, a volte, dimostrato che la sede principale dell'operatore economico che fornisce un qualsiasi servizio nel settore ICT e, conseguentemente, la sede in cui i dati vengono conservati hanno una importanza dirimente per gli equilibri geopolitici. Stati Uniti e Cina su tutte ne costituiscono un esempio lampante: il fatto che i più grandi operatori privati OTT siano nati

Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

28. DellaMorte 2018, p. 135; Aktoudianakis 2020, p. 3.
29. Ferracane 2017, spec. pp. 2-3.
30. Ryan-Falvey-Merchant 2013.
31. Ad esempio, Savelyev 2016 tratta il caso della Russia.
32. Polatin-Reuben-Wright 2014.
33. Boncinelli 2021, spec. p. 41.
34. Ferracane 2017, spec. p. 6.
35. Chander-Lê 2015; Castro 2013.
36. Chander-Lê 2015.
37. Bauer-LeeMakiyama-Van der Marel-Verschelde 2014; Chander-Lê 2015, spec. pp. 713-739; Castro 2013.

e abbiano la sede principale in detti Paesi fa sì che i rispettivi governi siano in una posizione di gran lunga più favorevole per beneficiare – di riflesso o per imposizione normativa – del potere garantito dal controllo del mezzo tecnico.

Quanto agli Stati Uniti, sono numerosi gli episodi che testimoniano la fondatezza di tale assunto. Si pensi alla nota prassi diffusa fra le autorità pubbliche di chiedere accesso alle informazioni detenute da imprese private[38]; all'ormai celeberrimo caso *Datagate* relativo alle rivelazioni dell'ex dipendente della CIA, Edward Snowden, concernenti il programma di sorveglianza di massa attuato dagli Stati Uniti[39]; o, da ultimo, all'entrata in vigore nel 2018 del *Clarifying Lawful Overseas Use of Data Act*, noto come *Cloud Act*, il quale impone agli *electronic communications services providers* e ai *remote computing service providers* di consentire alle sole autorità americane l'accesso ai dati relativi agli utenti indipendentemente dal luogo in cui tali informazioni sono localizzate[40].

Parimenti, l'ordinamento giuridico della Repubblica popolare cinese, oltre a consentire alla pubblica autorità l'accesso alle informazioni nella disponibilità di soggetti privati[41], ha coniato i concetti di *important data* e di *national core data* al fine di assicurare un maggiore controllo pubblico su informazioni che vantano uno stretto legame con la sicurezza nazionale, lo sviluppo economico e gli interessi del Paese[42].

Innanzi al progressivo consolidamento di tale quadro fattuale, caratterizzato da una accesa frizione tra diritto e tecnologia e da una progressiva concentrazione di potere in capo a entità pubbliche e private localizzate all'infuori del territorio europeo, l'Unione europea ha intrapreso un lento cammino di riforme volto a rielaborare l'architettura dell'ordinamento continentale in materia di protezione e circolazione dei dati personali e non personali[43].

Tale percorso, ancora *in itinere*, ha di recente raggiunto due traguardi di estrema rilevanza, i quali rappresentano, in un certo senso, una prima e rilevante risposta del legislatore innanzi ai mutamenti economico-sociali di cui si è detto. Si tratta, da un lato, del *Data Governance Act*[44], e, dall'altro, dal *Data Act*[45].

Il paragrafo che segue si concentrerà sul secondo di questi atti normativi allo scopo di comprendere se la nuova direzione intrapresa dal legislatore eurounitario si inserisce nel solco di quelle iniziative riconducibili alle politiche di *Data Nationalism* come sopra delineate.

4. Il *Data Act* tra sovranità digitale, accesso e circolazione dei dati

Per trovare una risposta al quesito che ha stimolato la redazione del presente scritto occorre svolgere una breve premessa utile a comprendere se la volontà del legislatore europeo sia effettivamente quella di promuovere una politica di protezionismo delle proprie informazioni, limitando (ulteriormente) la circolazione dei dati al di fuori del territorio continentale.

38. Cate-Kuner-Millard-Svantesson 2014. Anche se non mancano casi di operatori che si sono opposti a tale prassi, si vedano al riguardo Rubechi 2016, spec. p. 23; Orofino 2016.
39. Nino 2013.
40. Cantekin 2018; Christakis-Terpan 2021.
41. Wang 2012.
42. Pagnanelli 2021, spec. pp. 20-21.
43. Per una puntuale ricostruzione della evoluzione della disciplina in materia di protezione dei dati personali, si veda Calzolaio 2017; per una disamina della disciplina europea in materia di dati non personali, sia consentito rinviare a Torregiani 2020.
44. Si tratta del Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (*Regolamento sulla governance dei dati*).
45. Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (*regolamento sui dati*).

L'approvazione del Regolamento (UE) 2016/679 prima[46], e del Regolamento (UE) 2018/1807 poi[47], hanno plasmato un diritto dei dati europeo dicotomico in quanto costruito sulla distinzione tra i dati a carattere personale, ossia quelli riguardanti una persona fisica identificata o identificabile[48], e quelli non personali, che invece includono tutte le informazioni non rientranti nella prima categoria[49].

Il quadro normativo che ne è derivato si caratterizza per un evidente squilibrio tra le due categorie di dati, giacché, se da un lato i dati a carattere personale sono oggetto di una articolata e capillare regolazione, dall'altro, la fattispecie dei dati non personali non ha ricevuto, quantomeno nel 2018, pari attenzione da parte delle istituzioni europee.

Tale sviluppo si è tradotto in un profondo divario anche con riguardo ai due corrispondenti regimi di circolazione dei dati: se i dati personali possono uscire dai confini europei solo nel rispetto delle stringenti condizioni previste dal capo V del GDPR[50], per quelli non personali il Regolamento (UE) 2018/1807 ha cercato di liberalizzare la circolazione all'interno dei confini continentali, ma ha totalmente tralasciato la dimensione relativa alla circolazione esterna di queste informazioni[51].

L'assetto ordinamentale così formatosi è sin da subito parso troppo distante dalla realtà fattuale del mondo digitalizzato, sia perché prescinde dalle difficoltà di procedere a una esatta distinzione fra dati personali e non[52], sia perché sottovaluta colpevolmente l'impatto che il trattamento dei dati a carattere non personale può avere sulla società e sulla sovranità dell'Unione[53].

Queste, in estrema sintesi, sono le premesse dalle quali muove il *Data Act*[54]: il testo del provvedimento rappresenta un interessante indicatore della presa di coscienza da parte dell'Unione delle carenze del proprio impianto ordinamentale e dei mutamenti che investiranno il diritto europeo dei dati negli anni a venire.

In proposito, il *Data Act* e l'altro regolamento recentemente approvato, il *Data Governance Act*, costituiscono provvedimenti normativi tra loro comunicanti e il cui scopo ultimo risiede nella creazione di un nuovo modello "europeo" di governance dei dati quale strumento utile, da un lato, a rallentare l'accumulo esponenziale di potere in capo ai soggetti, pubblici e privati, esterni all'Unione e, dall'altro, a proteggere la sovranità degli Stati membri anche attraverso la riduzione della quantità dei dati che, fuoriuscendo dal territorio europeo,

46. Si tratta del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati o, dall'acronimo inglese, GDPR).
47. Si tratta 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.
48. Così recita l'art. 4, punto 1) del GDPR.
49. L'art. 3, punto 1) del Regolamento (UE) 2018/1807 li definisce come «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679».
50. Nello specifico, gli articoli dal 44 al 50 del GDPR prevedono come condizione per il trasferimento dei dati al di fuori dell'Unione europea, una tra le seguenti: una decisione di adeguatezza della Commissione europea; la predisposizione di garanzie adeguate; il ricorso a norme vincolanti d'impresa; un accordo internazionale per le decisioni di autorità estere; la sussistenza di una delle deroghe previste dall'art. 49 del GDPR.
51. Per una trattazione più approfondita, sia consentito rinviare a Torregiani 2021.
52. Montagnani 2019, pp. 311-313.
53. Per un approfondimento sia consentito rinviare a Torregiani 2021a.
54. Tra l'altro, è lo stesso testo del *Data Act* a rimarcare la necessità di integrare il Regolamento sui dati non personali, anche se con specifico riferimento al tema dei codici di condotta di autoregolamentazione per agevolare il passaggio a un diverso fornitore di servizi di trattamento dei dati e per la portabilità dei dati. In proposito, l'art. 1 par. 7 prevede espressamente che: «Il presente regolamento integra l'approccio di autoregolamentazione di cui al regolamento (UE) 2018/1807 aggiungendo obblighi di applicazione generale relativi al passaggio ad altri servizi cloud».

sono destinati a divenire una risorsa preziosa per un'autorità o un'industria extraeuropea.

A tal fine, il *Data Act* si pone in perfetta continuità con il *Data Governance Act*, giacché, a fronte di un obiettivo che può dirsi per certi versi unitario[55], dedica le sue prescrizioni ad ambiti in parte diversi rispetto al Regolamento (UE) 2022/868[56], nel tentativo di completare il disegno globale in materia di gestione dei dati generati in territorio europeo. In particolare, il *Data Act* inserisce una nuova gamma di diritti e di corrispondenti doveri al fine di agevolare l'accesso ai dati da parte dei soggetti più deboli del ciclo di raccolta e trattamento dei dati e da parte di enti pubblici che potrebbero necessitare delle informazioni detenute dai privati in particolari situazioni emergenziali. Conseguentemente, il Regolamento detta le condizioni e le modalità affinché i dati detenuti da chi fabbrica prodotti o offre servizi capaci di raccogliere e trattare informazioni siano messi a disposizione dell'utente o, su richiesta di quest'ultimo, di fornitori di servizi terzi, prescrivendo per diversi attori dell'attuale panorama dell'economia digitale nuove disposizioni in materia di trasferimento dei dati, validità delle clausole contrattuali e interoperabilità[57].

In sostanza, la sua funzione primaria appare essenzialmente quella di garantire una migliore allocazione del valore delle informazioni tra i differenti attori che intervengono nelle *value chains* dell'economia dei dati[58], avuto particolare riguardo ai dati generati o raccolti nel contesto dell'utilizzo di prodotti e servizi rientranti nell'ambito dell'*Internet of Things* o di servizi *cloud* e di trattamento dei dati generalmente intesi[59].

55. La parte introduttiva della proposta originaria del *Data Act* afferma espressamente che «La presente proposta integra l'atto sulla governance dei dati adottato di recente». In proposito, si veda la Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022, COM(2022) 68, p. 5.
56. Il *Data Governance Act* si focalizza, in particolare sui seguenti quattro profili: a) il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici; b) un quadro di notifica e controllo per la fornitura di servizi di intermediazione dei dati; c) un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici; d) un quadro per l'istituzione di un comitato europeo per l'innovazione in materia di dati – comitato che, tra l'altro, viene richiamato anche dall'art. 42 del *Data Act*. Per un approfondimento in materia di *Data Governance Act*, si veda Iannuzzi 2021.
57. L'obiettivo del *Data Act* è sintetizzato dal considerando n. 5, il quale recita: «Il presente regolamento garantisce che gli utenti di un prodotto connesso o di un servizio correlato nell'Unione possano accedere tempestivamente ai dati generati dall'uso di tale prodotto connesso o servizio correlato e che tali utenti possano utilizzare i dati, anche condividendoli con terzi di loro scelta. Esso impone ai titolari dei dati l'obbligo di mettere i dati a disposizione degli utenti e dei terzi scelti dagli utenti in determinate circostanze. Garantisce inoltre che i titolari dei dati mettano i dati a disposizione dei destinatari dei dati nell'Unione a condizioni eque, ragionevoli e non discriminatori e in modo trasparente. Le norme di diritto privato sono fondamentali nel quadro generale della condivisione dei dati. Il presente regolamento adegua pertanto le norme di diritto contrattuale e impedisce lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo. Il presente regolamento garantisce inoltre che i titolari dei dati mettano a disposizione degli enti pubblici, della Commissione, della Banca centrale europea o degli organismi dell'Unione, ove vi sia una necessità eccezionale, i dati necessari per lo svolgimento di un compito specifico nell'interesse pubblico. Il presente regolamento mira altresì ad agevolare il passaggio tra servizi di trattamento dei dati e a migliorare l'interoperabilità dei dati e dei meccanismi e servizi di condivisione dei dati nell'Unione. È opportuno non interpretare il presente regolamento come un atto che riconosce o che conferisce ai titolari dei dati un nuovo diritto di utilizzare i dati generati dall'uso di un prodotto connesso o di un servizio correlato».
58. European Commission 2021.
59. L'art. 1, par. 1 del *Data Act*, individua come oggetto del Regolamento «tra l'altro: a) la messa a disposizione dei dati del prodotto connesso e di un servizio correlato all'utente del prodotto connesso o del servizio correlato; b) la messa a disposizione di dati da parte dei titolari dei dati ai destinatari dei dati; c) la messa a disposizione di dati da parte dei titolari dei dati agli enti pubblici, alla Commissione, alla Banca centrale europea e a organismi

Per quanto di interesse ai fini del presente contributo, il capo II è dedicato alla condivisione dei dati da impresa a consumatore e da impresa a impresa e contiene le modalità attraverso cui i produttori debbono consentire agli utenti dei prodotti e dei servizi correlati, o ai terzi dagli stessi indicati, l'accesso ai dati generati durante l'utilizzo del prodotto o del servizio[60]; il capo III individua gli obblighi di messa a disposizione delle informazioni per i titolari dei dati[61]; il capo IV disciplina le clausole contrattuali abusive dirette a limitare illegittimamente l'accesso ai dati per altre imprese; il capo V indica le condizioni al verificarsi delle quali sussiste l'obbligo di mettere i dati a disposizione di enti pubblici; il capo VI regola il passaggio da un fornitore di servizi di trattamento dei dati a un altro; con il capo VII viene disciplinato l'accesso e il trasferimento dei dati non personali; mentre il capo VIII introduce le prescrizioni relative alla interoperabilità.

Dall'esame delle disposizioni presenti nei capi citati, appare evidente che il *Data Act* è destinato, in primo luogo, a incidere sul tema della proprietà dei dati industriali, ossia sull'ipotizzato riconoscimento di un diritto di proprietà concernente il bene immateriale "dato". Storicamente, le correnti della dottrina economico-giuridica che si sono contrapposte su questo campo hanno visto, da un lato, i fautori dell'introduzione di una privativa vera e propria e, dall'altro, i sostenitori di un differente approccio basato esclusivamente sul riconoscimento di un diritto di accesso in favore dei soggetti intervenuti nel processo di generazione del dato[62].

Con l'approvazione del *Data Act*, le istituzioni europee sembrano aver optato in maniera decisa per la seconda di queste alternative: si riconosce al soggetto debole del rapporto contrattuale nascente dall'utilizzo delle tecnologie digitali – l'utente/consumatore – un diritto di accedere alle informazioni dallo stesso generate, sì da compensare lo squilibrio di potere negoziale patito nei confronti delle grandi compagnie produttrici o fornitrici dei servizi, le quali solitamente hanno la capacità tecnica di escludere gli altri dall'accesso ai dati raccolti[63].

Ad uno sguardo più attento, nelle disposizioni del nuovo Regolamento è inoltre possibile intravedere la volontà dell'Unione di difendersi dagli attacchi alla propria *data sovereignty* provenienti dall'esterno.

dell'Unione, a fronte di necessità eccezionali per tali dati, per l'esecuzione di un compito specifico svolto nell'interesse pubblico; d) la facilitazione del passaggio da un servizio di trattamento dei dati all'altro; e) l'introduzione di garanzie contro l'accesso illecito di terzi ai dati non personali; e f) lo sviluppo di norme di interoperabilità per i dati a cui accedere, da trasferire e utilizzare».

60. L'art. 2 del *Data Act* definisce al punto 6) il "servizio correlato" come «un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso»; al punto 15) i "dati del prodotto" come i «dati generati dall'uso di un prodotto connesso e progettati dal fabbricante in modo tale che un utente, un titolare dei dati o un terzo, compreso se del caso il fabbricante, possano reperirli tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo»; e, al punto 16) i "dati di un servizio correlato" come i «dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore».
61. Il "titolare dei dati" viene definito dall'art. 2, punto 13) del *Data Act* come la «persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato».
62. Per un approfondimento si vedano Drexl 2016; Wiebe 2016.
63. Con riferimento alla cosiddetta escludibilità, ossia la possibilità di escludere gli altri dalla conoscenza di una determinata informazione tramite l'implementazione di misure tecniche *ad hoc* si veda Kerber 2016.

In primo luogo, il *Data Act* attribuisce agli utenti e alle imprese europee il diritto di ottenere l'accesso ad informazioni che altrimenti rimarrebbero nella esclusiva disponibilità delle grandi compagnie tecnologiche che, come detto, sono per la maggior parte locate al di fuori dei confini continentali[64]. Sotto tale profilo, il *Data Act* sembra porsi sul versante opposto rispetto a quegli atti normativi extra-europei, su tutti il *Cloud Act* statunitense[65], volti a consentire l'accesso a informazioni che potrebbero essere archiviate in server situati in territori rispondenti ad altre giurisdizioni[66].

In secondo luogo, la volontà del legislatore traspare in maniera ancor più evidente con riferimento all'obbligo per il titolare dei dati di mettere i dati in suo possesso a disposizione di terzi indicati dall'utente, come previsto dall'articolo 5 del *Data Act*. Il paragrafo terzo di tale disposizione esclude *expressis verbis* dal novero dei "terzi" riceventi quelli che vengono designati dalla Commissione europea come *gatekeepers*[67], i quali, ricoprendo la posizione di soggetti che dettano le condizioni per l'accesso al mercato[68], coincidono, in sostanza, con le *big tech* aventi sede in Paesi terzi[69]. In altri termini, in virtù di tale preclusione, i *gatekeepers* non possono vantare il medesimo diritto di ottenere i dati detenuti da altri operatori sulla base di una richiesta di trasferimento promossa dall'utente[70].

Dall'altro lato, invece, il *Data Act* concerne anche il versante relativo alla circolazione esterna dei dati non personali generati nel contesto

64. Eloquente in tal senso l'art. 1, par. 3 del *Data Act* che nel definire l'ambito di applicazione soggettivo del Regolamento stabilisce che: «Il presente regolamento si applica: a) ai fabbricanti di prodotti connessi immessi sul mercato dell'Unione e ai fornitori di servizi correlati, indipendentemente dal loro luogo di stabilimento di tali fabbricanti e fornitori; b) agli utenti nell'Unione di prodotti connessi o servizi correlati di cui alla lettera a); c) ai titolari dei dati, indipendentemente dal loro luogo di stabilimento, che mettono dati a disposizione dei destinatari dei dati nell'Unione; d) ai destinatari dei dati nell'Unione a disposizione dei quali sono messi i dati; e) agli enti pubblici, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione che chiedono ai titolari dei dati di mettere i dati a disposizione nel caso tali dati siano necessari a fronte di una necessità eccezionale per l'esecuzione di un compito specifico svolto nell'interesse pubblico e ai titolari dei dati che forniscono tali dati in risposta a tale richiesta; f) ai fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono tali servizi a clienti nell'Unione; g) ai partecipanti agli spazi di dati, ai venditori di applicazioni che utilizzano contratti intelligenti e alle persone la cui attività commerciale, imprenditoriale o professionale comporti l'implementazione di contratti intelligenti per altri nel contesto dell'esecuzione di un accordo».
65. Cerrina Feroni 2022.
66. Per un approfondimento in merito alle problematiche giuridiche legate al fenomeno cloud si veda Boncinelli 2021.
67. L'art. 5, par. 3 del *Data Act* si riferisce a «Qualsiasi impresa designata come gatekeeper a norma dell'articolo 3 del regolamento (UE) 2022/1925», il quale, a sua volta, prevede l'attribuzione di tale qualifica per le imprese che a) hanno un impatto significativo sul mercato interno; b) forniscono un servizio di piattaforma di base che costituisce un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali; c) detengono una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisiscano siffatta posizione nel prossimo futuro.
68. Contaldi 2021.
69. Gallese 2022.
70. Eloquente in tal senso il considerando n. 40 nella parte in cui afferma che «è emerso un piccolo numero di imprese molto grandi con un notevole potere economico nell'economia digitale, ottenuto grazie all'accumulo e all'aggregazione di grandi volumi di dati e all'infrastruttura tecnologica per la loro monetizzazione. Tali imprese molto grandi includono imprese che forniscono servizi di piattaforma di base che controllano interi ecosistemi di piattaforme nell'economia digitale e che gli operatori di mercato esistenti o nuovi non sono in grado di sfidare o contrastare. […] data la capacità inarrivabile di tali imprese di acquisire dati, l'inclusione dei gatekeeper quali beneficiari del diritto di accesso ai dati non è necessaria per conseguire l'obiettivo del presente regolamento, e sarebbe pertanto sproporzionata per i titolari dei dati soggetti a tali obblighi».

europeo, dunque quella dimensione colpevolmente rimasta senza disciplina nell'ambito del Regolamento (UE) 2018/1807.

L'articolo 32 del *Data Act* esordisce imponendo in capo ai fornitori di servizi di trattamento dei dati l'obbligo di adozione delle misure tecniche, organizzative e giuridiche necessarie a impedire l'accesso governativo internazionale di Paesi terzi ai dati non personali detenuti nell'Unione e il trasferimento di detti dati in tutte le ipotesi in cui tali operazioni dovessero contrastare con il diritto eurounitario o degli Stati membri[71].

Nel caso in cui il trasferimento sia richiesto da decisioni o sentenze di un organo giurisdizionale o di un'autorità amministrativa di un Paese terzo, i paragrafi successivi dell'articolo citato condizionano il trasferimento alla sussistenza di un accordo internazionale o, in assenza di questo, al rispetto di una serie di guarentigie fra le quali compaiono la motivazione e la proporzionalità della richiesta, l'esame dell'opposizione eventualmente sollevata dal soggetto richiesto e l'obbligo di tenere in considerazione gli interessi di quest'ultimo[72].

In tal senso, il *Data Act* ribadisce quanto già disposto dal *Data Governance Act* in materia di trasferimento di dati non personali, indirizzando disposizioni nella sostanza simili verso la particolare categoria dei fornitori di servizi di trattamento di dati[73].

Anche in quest'ottica, dunque, tanto il *Data Governance Act* quanto il *Data Act* costituiscono una chiara risposta del legislatore europeo alla entrata in vigore di atti normativi esteri capaci di ridurre la sovranità sui dati europei. Le preoccupazioni relative all'accesso illecito da parte delle amministrazioni pubbliche di Paesi terzi[74], hanno condotto a un cambiamento di impostazione consistente nella trasposizione dei principi e delle regole stabiliti dal capo V del GDPR, che già di per sé costituivano una misura di *data localization*, nel diverso ambito dei dati non personali.

Dalle norme testé esaminate emerge in maniera chiara la volontà delle istituzioni europee di procedere verso la creazione di un sistema che permetta all'Unione di mantenere un maggiore controllo sulle sorti dei dati generati in ambito continentale. Fra le righe del *Data Act* è possibile scorgere una accentuazione di quella tendenza alla localizzazione dei dati all'interno dell'Unione europea inaugurata con l'entrata in vigore del GDPR per le informazioni a carattere personale. Oltre al rinnovato rilievo assunto dalla categoria dei dati non personali in seno ai due regolamenti più recenti, le disposizioni in tema di accesso e di trasferimento consentono di collocare il *Data Act* all'interno del novero delle politiche normative riconducibili al fenomeno del *Data Nationalism*.

Con tale provvedimento, il legislatore punta infatti alla limitazione del potere di ingerenza esercitato dagli attori esterni al circuito eurounitario attraverso un duplice meccanismo di esclusione. Da un lato, viene varata una normativa che preclude espressamente i benefici del diritto di accesso per quei soggetti privati che, secondo la valutazione della Commissione europea, sono in grado di alterare gli equilibri di mercato e che, allo stato attuale, risiedono tutti negli Stati Uniti o nella

71. A norma dell'art. 2, punto 8) del *Data Act*, il "servizio di trattamento dei dati" consiste in un «un servizio digitale fornito a un cliente e che consente l'accesso di rete universale e su richiesta a un pool condiviso di risorse informatiche configurabili, scalabili ed elastiche di natura centralizzata, distribuita o altamente distribuita e che può essere rapidamente erogato e rilasciato con un minimo sforzo di gestione o interazione con il fornitore di servizi»; per una descrizione più dettagliata, si vedano i considerando 80 e 81. A titolo esemplificativo, si segnala che in tale categoria rientrano i servizi di servizi *cloud* ed *edge computing*.

72. Art. 32, parr. 2 e 3 del *Data Act*.

73. L'art. 31 del Regolamento (UE) 2022/868 (*Data Governance Act*) prescrive le medesime condizioni e obblighi per l'accesso e il trasferimento internazionale dei dati non personali quando coinvolge enti pubblici, titolari del diritto di riutilizzo dei dati, fornitori di servizi di intermediazione dei dati e organizzazioni per l'altruismo dei dati.

74. Già la Proposta di *Data Act* affermava nella parte introduttiva che: «sono state espresse preoccupazioni in merito all'accesso illecito ai dati da parte di amministrazioni pubbliche di paesi terzi/esterni allo Spazio economico europeo (SEE)», p. 3.

Repubblica popolare cinese[75]. Dall'altro lato, il *Data Act* ha introdotto ulteriori obblighi di localizzazione di dati con riguardo ad una categoria di informazioni che prima, salvo specifiche normative di settore, poteva liberamente lasciare il territorio dell'Unione, mentre ora – o meglio, quando il *Data Act* diverrà applicabile[76] – impedisce l'indiscriminato e massivo trasferimento internazionale di dati non personali.

5. Considerazioni conclusive: tra prospettive di sviluppo e rischio di isolazionismo

L'ingresso nell'era digitale ha scatenato una feroce competizione per il controllo dei dati poiché da tale controllo passa il mantenimento o l'acquisizione della sovranità degli Stati e delle organizzazioni internazionali. Se gli operatori privati agiscono muovendosi sul piano prettamente tecnico attraverso la realizzazione di infrastrutture e di sistemi tecnologici in grado di rendere sempre più profittevole il trattamento dei dati, le entità pubbliche hanno intrapreso una battaglia che si combatte soprattutto a colpi di atti normativi.

In questo senso, i recenti sviluppi dell'ordinamento europeo dei dati, culminati con l'entrata in vigore del *Data Act*, dimostrano che l'intenzione del legislatore europeo va al di là del semplice rafforzamento del mercato unico, come imporrebbe la base giuridica su cui vengono fondati quasi tutti i provvedimenti legislativi in materia[77]. Il *Data Act*, così come il *Data Governance Act*, sembrano infatti essere stati concepiti come strumenti utili anche alla realizzazione di un modello "europeo" di gestione dei dati, e delle tecnologie digitali in generale, la cui finalità ultima risiede nella difesa della sovranità continentale.

Pertanto, se, da una parte, il *Data Act* mira a incentivare la concorrenzialità e lo sviluppo di prodotti e servizi maggiormente innovativi aumentando la disponibilità e la condivisione dei dati all'interno dell'Unione, dall'altra parte, lo stesso provvedimento fa parte di una strategia finalizzata a respingere gli attori extra-europei per mezzo di un irrigidimento dei confini digitali del vecchio continente.

Sotto il profilo del *Data Nationalism*, il *Data Act* non rappresenta una vera rottura rispetto alla strada già tracciata in precedenza dalla stessa Unione, la quale già da tempo aveva introdotto un meccanismo condizionale per il trasferimento dei dati personali all'estero, ma contribuisce di certo al decremento della fuoriuscita della ulteriore categoria dei dati non personali, che nell'epoca attuale si è dimostrata essere di vitale importanza.

Sebbene l'innalzamento delle barriere digitali europee possa apparire un approccio comprensibile nel contesto storico attuale e possa effettivamente risultare funzionale a un utile posizionamento nello scacchiere globale, la sovranità digitale, specie per una entità tecnologicamente fragile come l'Unione europea, passa anche attraverso due tasselli fondamentali: la riduzione della dipendenza da infrastrutture estere per la gestione dei dati e la cooperazione internazionale finalizzata alla promozione di un approccio comune alla regolazione delle nuove tecnologie[78].

L'Unione dovrebbe pertanto ispirarsi ad una idea di sovranità digitale "aperta" dove riescono a trovare spazio anche partner esterni che sono in grado di fornire quelle competenze e quegli strumenti di cui la realtà continentale attualmente non dispone e deve altresì investire in misura più incisiva sulla effettiva realizzazione di una infrastruttura digitale di matrice europea capace di competere con i concorrenti americani e cinesi. Al contrario, insistere solamente su misure normative ispirate al *Data Nationalism*, trascurando le altre dimensioni rilevanti, non farà altro che alimentare un deleterio "isolazionismo digitale", in cui gli attori

75. Con il primo atto di designazione adottato il 6 settembre 2023, la Commissione europea ha infatti qualificato come *gatekeepers* le seguenti sei piattaforme digitali: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft. Si veda in proposito il comunicato stampa.

76. Ai sensi dell'art. 50, le disposizioni del *Data Act* diverranno applicabili a decorrere dal12 settembre 2025.

77. È bene infatti notare che sia il *Data Act* sia il *Data Governance Act* sono adottati sulla base dell'art. 114 TFUE, che attribuisce al Parlamento ed al Consiglio la competenza normativa per 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.

78. Aktoudianakis 2020.

pubblici e privati rimangono in un circuito chiuso e non comunicante con l'esterno, il quale, in ultima analisi, non potrà che condurre l'Unione verso una prevedibile disfatta.

Riferimenti bibliografici

A. Aktoudianakis (2020), *Fostering Europe's Strategic Autonomy - Digital sovereignty for growth, rules and cooperation*, in European Policy Centre, 2020

M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde (2014), *The cost of data localisation: friendly fire on economic recovery*, ECIPE Occasional Paper No. 3/2014

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

V. Boncinelli (2021), *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in "Rivista italiana di informatica e diritto", 2021, n. 1

A. Buratti (2022), *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?* in "Media-Laws", 2022, n. 2

S. Calzolaio (2017), *Protezione dei dati personali*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017

K. Cantekin (2018), *Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?*, in "Eurojus.it, Big data and Public Law: new challenges beyond data protection", Numero speciale, 2018

F.H. Cate, C. Kuner, C. Millard, D.J. Svantesson (2014), *Systematic Government Access to Private-Sector Data Redux*, in "International Data Privacy Law", vol. 4, 2014, n. 1

G. Cerrina Feroni (2022), *Luci e ombre della Data Strategy europea*, intervento del 13 maggio 2022 (Doc-Web9769786)

A. Chander, U.P. Lê (2013), *Data Nationalism*, in "Emory Law Journal", vol. 64, 2015, n. 3

D. Castro (2013), *The False Promise of Data Nationalism*, Information Technology & Innovation Foundation, 2013

T. Christakis, F. Terpan (2021), *EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in "International Data Privacy Law", vol. 11, 2021, n. 2, 2021

G. Contaldi (2021), *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in "Ordine internazionale e diritti umani", 2021, n. 2

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

R. Creemers (2020), *China's conception of cyber sovereignty: rhetoric and realization*, in D. Broeders, B. van den Berg (eds.), "Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics Lanham", Rowman & Littlefield, 2020

E. Cremona (2021), *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in "Osservatorio sulle fonti", 2021, n. 2

G. Della Morte (2018), *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, Editoriale Scientifica, 2018

J. Drexl (2016), *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in "Max Planck Institute for Innovation & Competition", Research Paper No. 16-13, 2016

European Commission (2021), *Inception Impact Assessment*, Ref. Ares(2021)3527151, 28 May 2021

M.F. Ferracane (2017), *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper, 2017, n. 1

C. Gallese (2022), *A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*, in "MediaLaws", 2022, n. 3

G. Gardini (2021), *Le regole dell'informazione. Verso la Gigabit Society*, Giappichelli, 2021

G. Gonzalez Fuster (2014), *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014

D. Kalff, A. Renda (2019), *Hidden Treasures. Mapping Europe's sources of competitive advantage in doing business*, Centre for European Policy Studies, 2019

W. Kerber (2016), *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, MAGKS Joint Discussion Paper Series in Economics, 2016, n. 37

A. Iannuzzi (2021), *La* governance *europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

M. Martoni (2020), *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in "federalismi.it", 2020, n. 1

M.L. Montagnani (2019), *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

M. Nino (2013), *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

M. Orofino (2016), *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, in "Diritto Pubblico Comparato ed Europeo", 2016, n. 2

V. Pagnanelli (2021), *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in "Rivista italiana di informatica e diritto", 2021, n. 1

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

D. Polatin-Reuben, J. Wright (2014), *An Internet with BRICS characteristics: data sovereignty and the Balkanisation of the Internet*, Usenix, 2014

C. Polito (2021), *La* governance *globale dei dati e la sovranità digitale europea*, in "IAI Papers", 2021, n. 11

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

P.S. Ryan, R. Falvey, S. Merchant (2013), *When the Cloud Goes Local: The Global Problem with Data Localization*, in "Computer", vol. 46, 2013, n. 12

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

A. Savelyev (2016), *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, in "Computer Law & Security Review", vol. 32, 2016, n. 1

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

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

T. Streinz (2021), *The Evolution of European Data Law*, in P. Craig, G. de Búrca (eds.), "The Evolution of EU Law", Oxford University Press, 2021

G. Surblyte (2016), *Data as a Digital Resource*, in "Max Planck Institute for Innovation & Competition Research", Paper No. 16-12, 2016

S. Torregiani (2021), *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Torregiani (2021a), *L'impatto dei dati non personali sulle decisioni algoritmiche: la prospettiva delle autorità amministrative indipendenti europee*, in "Osservatorio sulle fonti", 2021, n. 2

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18

J. Van Dijck (2020), *Governing digital societies: Private platforms, public values*, in "Computer Law & Security Review", vol. 36, 2020

J. Van Dijck (2014), *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in "Surveillance and Society", vol. 12, 2014, n. 2

Z. Wang (2012), *Systematic government access to private-sector data*, in "China International Data Privacy Law", vol. 2, 2012, n. 4

A. Wiebe (2016), *Protection of industrial data – a new property right for the digital economy?*, in "Journal of Intellectual Property Law & Practice", 2016

V. Zeno-Zencovich (2016), *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), "La protezione transnazionale dei dati personali. Dai 'Safe Harbour Principles' al 'Privacy Shield'", RomaTre-press, 2016

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0130 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Erik Longo

La ricerca di un'antropologia costituzionale della società digitale

Questo articolo approfondisce le complessità che circondano l'utopia di Internet, esaminando le sue implicazioni per la democrazia, il dato-centrismo e le sfide normative nell'ecosistema digitale. Esplora le trasformazioni apportate dalle più recenti tecnologie digitali, concentrandosi sul loro impatto sul diritto costituzionale e sulle strutture sociali. L'articolo fa parte di una sezione monografica sull'"utopia di Internet" e sulle sfide della regolamentazione e della gestione dello spazio digitale. L'articolo evidenzia la necessità di una comprensione sfumata di questi temi nel contesto del diritto costituzionale e dei cambiamenti antropologici del XXI secolo.

Datificazione – Dataismo – Data-justice – Trasparenza algoritmica – Controllo umano

The quest for a constitutional anthropology of the digital society

This article delves into the complexities surrounding the utopia of the internet, examining its implications for democracy, data-centrism, and the regulatory challenges in the digital ecosystem. It explores the transformation brought about by the most recent digital technologies, focusing on their impact on constitutional law and societal structures. The paper is part of a monographic section on the "utopia of the Internet" and the challenges of regulating and managing the digital space. The article highlights the need for a nuanced understanding of these issues within the context of constitutional law and the anthropological changes of the 21st century.

Datafication – Dataism – Data-justice – Algorithmic transparency – Human oversight

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

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. La "fine di Internet": la sfida

Questa sezione monografica della *Rivista italiana di informatica e diritto* prende corpo intorno a un'idea allettante: smontare ciò che rimane della c.d. utopia di Internet. Il tema è molto noto, anche se in pochi si sono cimentati a individuare i fili rossi che legano, o slegano, l'evoluzione della rete dalle idee che avevano portato un gruppo di scienziati tra gli anni Settanta e Ottanta a immaginarsi una forma alternativa di comunicazione che fosse legata a dinamiche di rete. Simone Calzolaio nell'introduzione a questa sezione, molto acutamente, rileva uno scarto.

«La rete Internet doveva renderci più liberi, più informati e più consapevoli, più uniti in un unico piccolo mondo, più tutelati e più sicuri rispetto agli altri umani, ai poteri pubblici e ai poteri privati. La rete Internet doveva essere il nuovo stadio e forse anche l'ulteriore inedito lascito delle liberaldemocrazie al mondo. Le cose stanno andando – come per tutte le utopie – molto diversamente. L'avvento e l'evoluzione della rete Internet sono ormai divenute il terreno di una nuova era della regolazione giuridica: l'esigenza di governo della sfuggente società dei dati. Proviamo […] a passare in rassegna – con la piena consapevolezza che la materia di studio è più grande delle capacità di ciascuno – quali sono alcuni dei nuovi ambiti e dei nuovi strumenti di questa sfida regolatoria, da una prospettiva schiettamente liberaldemocratica»[1].

I saggi qui raccolti si propongono di reagire a questa provocazione. Risposta non facile, se si pensa che la materia che forma l'oggetto di questa ricerca risulta oggetto di numerose indagini da parte di studiosi non solo di diritto ma di altre discipline, come la sociologia, la filosofia, la politologia e chiaramente l'economia. Non mi sembra, perciò, errato ricordare che i temi qui affrontati si caratterizzano per la loro natura di frontiera e per l'essere diretti a investigare realtà ancora non ben inquadrabili, che gli Stati e le organizzazioni internazionali stentano a regolare per la velocità con cui tale realtà si va trasformando sotto la spinta del progresso scientifico e dell'innovazione tecnologica. Neanche l'opinione pubblica o la politica percepisce e padroneggia pienamente gli avanzamenti che fanno della Rete un ambiente nuovo e rivoluzionario per le nostre vite quotidiane. Si pensi, in questo senso, al dibattito recente – paradigmatico – sulla regolazione dei prodotti con Intelligenze Artificiali, sia in Europa che in altre parti del mondo.

Ciò che oggi sappiamo di tali problemi lo individuano ancora le parole di Calzolaio quando sottolinea – e, ragionevolmente, si aspetta – l'arrivo di una «nuova era della regolazione giuridica» che dovrà governare la «sfuggente società dei dati».

Per giungere a inquadrare tali questioni, i saggi della sezione monografica si confrontano con materie ancora fluide sul piano dell'esperienza concreta: società dei dati, datificazione, disinformazione, cybersicurezza, *online dispute resolutions*, ecc. Argomenti che fanno parte di un universo tecnologico in divenire, che il giurista stenta a cogliere, e che si prestano poco ad essere inquadrati nelle categorie della scienza giuridica[2].

1. Calzolaio 2023, p. [2].
2. Un esempio paradigmatico è certamente la "sovranità", come ricorda Gatti 2019.

Gli ultimi dieci anni sono stati un punto di passaggio decisivo per l'umanità. Possiamo dare per assodato che non viviamo più nell'assetto geopolitico costruito dopo la Seconda guerra mondiale e che sono cambiate le tecnologie alle quali avevamo affidato la produzione della ricchezza dopo la rivoluzione industriale. Sebbene il secolo attuale abbia ancora in sé molte caratteristiche del passato, ci siamo allontanati grandemente dalla società del secolo scorso, aprendoci a una serie di novità che nella maggior parte dei casi sono addirittura distruttive della realtà precedente.

Il fattore che ha più di tutti rappresentato il punto di oscillazione verso la nuova società e il nuovo assetto mondiale del nuovo millennio è certamente la pandemia da COVID-19. Quel periodo ha segnato un salto di realtà, rendendo tutti consapevoli di una mutazione antropologica in fermento da almeno trenta anni[3].

La pandemia ha altresì fatto emergere i problemi che da qualche anno erano sempre più evidenti in ragione del rapido avanzamento tecnologico, della trasformazione "tecnocratica" del potere e della fine della globalizzazione[4]. Al tecno-ottimismo si è affiancata una nuova forma di tecno-nichilismo[5], già serpeggiante e nota almeno a partire dalle crisi dei mutui subprime scoppiata nel 2008. Troviamo adesso una chiave di lettura unitaria e un filo argomentativo che possa aiutarci a mettere a fuoco i saggi.

2. Dato-centrismo

Il principale fattore di cambiamento rispetto al passato riguarda la "dimensione" dei dati. La società contemporanea è definibile essenzialmente a partire dal fenomeno "datificazione" o "datizzazione"[6], adattando il più corretto neologismo inglese *datafication*[7]. Non possiamo che subire l'impatto dei dati o come soggetti attivi che creano dati ovvero come individui che con le loro azioni producono dati che vengono usati per motivi di governance pubblica o privata. «In un mondo deterritorializzato e asincrono», come ha indicato recentemente Davide Bennato, «la tecnologia gioca un ruolo di connessione sociale assolutamente straordinario, ben più di qualche tempo fa»[8]. Abbiamo affidato alla tecnologia dei dati la mediazione sociale. Ancora Bennato fa notare: «(se) per creare uno spazio comune serve uno spazio digitale (…) e se per creare l'illusione della sincronizzazione abbiamo bisogno delle tecnologie in grado di gestire l'asincronia (…), allora la tecnologia diventa quello strumento che serve per gestire questa complessità sociale di cui essa non è né causa né effetto, ma "semplicemente" strumento abilitante»[9].

3. Tra i primi ad aver colto il salto, tra gli studiosi di diritto, vi è Simoncini 2020a.
4. Giaccardi-Magatti 2022.
5. Castells 2019.
6. Calzolaio 2017, pp. 594-635.
7. Il termine "datafication" è stato introdotto in un volume del 2013 sui processi di "big data" nelle imprese e nelle scienze sociali scritto da Mayer-Schönberger-Cukier 2013. Secondo gli autori «datare un fenomeno significa metterlo in forma quantificata in modo che possa essere tabulato e analizzato» (nostra la traduzione a p. 78). La *datafication*, sostengono gli autori, implica molto di più della conversione di materiale simbolico in forma digitale, poiché è la *datafication*, non la digitalizzazione, che «ha reso il testo (digitale) indicizzabile e quindi ricercabile» (p. 84). Attraverso questo processo, ampi settori della vita umana sono diventati suscettibili di essere elaborati attraverso forme di analisi che possono essere automatizzate su larga scala. Diventa, perciò, evidente la dinamica che guida la *datafication* come processo sociale: la spinta a «rendere (…) il comportamento umano (…) in una forma analizzabile» in un processo che era già stato definito come «la datafication di tutto» (pp. 93-94). In questo senso tali teorie sono una evoluzione del più complesso fenomeno della "non causalità" come elemento chiave della nuova scienza dei dati. Avendo a disposizione enormi quantità di dati è possibile giungere a una «interpretazione senza una teoria», basta utilizzare la correlazione statistica per estrarre senso dai dati a disposizione in assenza di una teoria. Su questo aspetto si v. l'oramai storico articolo di Anderson 2008. Il fenomeno è spiegato in maniera molto efficace da Pearl-Mackenzie 2018; Lycett 2013; Van Dijck 2014.
8. Bennato 2022, p. 12.
9. *Ivi*, pp. 12-13.

Fin dagli albori del Web 2.0 è stato sostenuto il potenziale civico dei nuovi social media e, sebbene la realtà abbia poi smorzato le previsioni più ingenue di una palingenesi politica della Rete, molti continuano a considerare queste tecnologie come la migliore speranza che ha l'umanità per espandere la democrazia globale, la libertà, l'uso della ragione e la solidarietà[10]. In fondo è sempre questo mantra di liberazione ad essere messo in luce a ogni nuovo avanzamento tecnologico[11], di cui l'utopia della Rete era stata forse la più lucida ed evoluta esperienza[12].

Solo dieci anni fa, i leader di Google Eric Schmidt e Jared Cohen ci assicuravano che, con così tante persone connesse in così tanti luoghi, il futuro ci avrebbe fatto guadagnare una «società civile più attiva, schietta e globalizzata» come mai il mondo avrebbe conosciuto. I nuovi cittadini e cittadine globali non solo sarebbero stati attivi e sani, ma anche informati, illuminati e impegnati in modo efficace nella costruzione di istituzioni civiche migliori.

La rivoluzione dei dati avrebbe portato benefici incalcolabili ai cittadini del futuro, una visione senza precedenti di come le altre persone pensano, si comportano e aderiscono alle norme o se ne discostano, in ogni società del mondo. La ritrovata capacità di ottenere informazioni accurate e verificate online, facilmente, nella propria lingua madre e in quantità infinita, avrebbe inaugurato una nuova era del pensiero critico nelle società di tutto il mondo (anche in quelle che prima erano culturalmente isolate). Quasi come fosse l'alba di un nuovo illuminismo.

Nelle società in cui le infrastrutture fisiche erano deboli, la connettività avrebbe consentito alle persone di creare nuove imprese, di impegnarsi nel commercio online e di interagire con il proprio governo a un livello completamente nuovo. La partecipazione dei cittadini avrebbe raggiunto il suo massimo storico, perché chiunque fosse stato in possesso di uno smartphone e dell'accesso a Internet, sarebbe stato in grado di svolgere un ruolo nella promozione della responsabilità e della trasparenza[13].

La verità, tuttavia, è che il nuovo ecosistema *data-centric* ha usato fino ad ora le informazioni generate per sorvegliare, controllare, manipolare e creare valore a favore di pochi[14], e non sappiamo come costringere a redistribuire questa ricchezza né come farne un elemento per la costruzione della pace anziché dell'innesco di nuove guerre[15]. Oggi, il tradimento dell'utopia ha reso la Rete più simile a un imponente software di gestione e ottimizzazione delle relazioni tra clienti e aziende anziché un fattore di democratizzazione[16].

Tutto ciò non è accaduto magicamente[17], ma grazie al fatto che la tecnica ha iniziato a funzionare non più solo come un sistema a disposizione della ragione umana teso ad interagire sul mondo al fine di modificarlo o a risolvere problemi in direzione del progresso, ma è divenuta il mondo che abitiamo[18]; un mondo dove sensori, oggetti connessi, dati, algoritmi e miriadi di sistemi informatici tra di loro connessi permeano e dominano i

10. Abbiamo provato a parlare di questi aspetti in Longo 2019.
11. Formenti 2010.
12. È nota l'affinità quasi elettiva – tanto sul piano organizzativo, quanto sul piano dei valori politico-culturali – fra le prime comunità online e nuovi movimenti politici, così come è stato ben sottolineato sul piano sociologico il ruolo svolto da Internet nell'organizzazione e nella crescita dei movimenti eco pacifisti, del movimento *no global*, del femminismo, ecc., come già sottolineava Castells 2006.
13. Wallace 2021.
14. Celebre è la ricostruzione di Zuboff 2019. Molto interessante lo studio condotto da Bakir-Laffer-McStay 2023, sui limiti etici della *data monetization*.
15. Acemoglu-Johnson 2023.
16. Barra-Sartori 2022.
17. L'idea che un artefatto tecnologico riesce ad imporsi quasi per magia è stata consacrata nella famosa frase di Clarke 1962 «qualunque tecnologia sufficientemente sofisticata è indistinguibile dalla magia». Si tratta ovviamente di una frase che nella sua iperbolicità apre esattamente verso il senso opposto di quanto essa esprima.
18. Balbi 2022.

nostri corpi[19], fino a renderli «una parte integrante del regno delle merci, degli spettacoli e delle informazioni»[20].

Da questa sintetica e superficiale descrizione derivano numerose conseguenze sociali, economiche e giuridiche. L'attuale ecosistema digitale si è fuso con l'ideologia dei social media, creando una nuova centralità strategica dei dati ma anche numerosi problemi[21]. Traendo spunto dai saggi di questo numero vorrei sottolineare la conseguenza più preoccupante della datificazione.

3. Dataismo

Il *dataism* (o anche *dataismo*), inteso come un «atteggiamento mistico nei confronti dei dati»[22], è il lato oscuro della società dei dati. Il termine, pur essendo stato elaborato fin dagli anni Dieci[23], ha preso forma a partire da una nota pagina del volume *Homo Deus* dello storico israeliano Yuval Harari[24]. Per quest'ultimo, a differenza del passato, la *datafication* ha portato a una "metafisica del dato": come i sostenitori del mercato libero credono nella mano invisibile del mercato, allo stesso modo i dataisti (così possiamo descrivere i propugnatori di questa ideologia) crederebbero nella mano invisibile del flusso dei dati. Tutto ciò che può essere convertito in dati è legittimo, così come è legittimo che i dati siano alla base del modo attraverso cui gestire la società di cui facciamo parte[25] (un presupposto sul quale potremmo aprire un dibattito infinito).

L'ideologia del dataismo mostrerebbe, quindi, le caratteristiche di una convinzione diffusa nella quantificazione oggettiva e nel potenziale tracciamento di tutti i tipi di comportamento umano o sociali attraverso le tecnologie dei media online e implicherebbero pure la fiducia negli agenti (istituzionali) che raccolgono, interpretano e condividono i dati raccolti dai social media, dalle piattaforme e da altre tecnologie di comunicazione[26].

Il problema di una società basata solo sui dati è il suo scadere immediato in una "totalitarian dimension", come ha sottolineato tra i primi il filosofo coreano Byung-Chul Han[27]. Non si tratta solo di un *totalitarismo cibernetico*, ovvero la sottoposizione dell'umanità alla diffusione dei software, ma della trasformazione di quello che è una «convenzione sociale strutturata e irrigidita dalla e nella tecnologia» in un "costrutto" che ha la pretesa della naturalità[28]. Questo modo di intendere la società dei dati, nel momento in cui attribuisce ai dati stessi una potenza salvifica e "soluzionistica", non considera che gli strumenti tecnologici, in quanto costruiti da esseri umani, non sono neutrali e non sono infallibili. È per questo che con molta lungimiranza il legislatore europeo ha previsto nell'art. 22 del GDPR che non è possibile essere sottoposti a una decisione completamente automatizzata dalla quale derivano conseguenze per la persona dell'interessato[29], e che il nuovo regolamento europeo sull'intelligenza artificiale si riferisce alla necessità dello *human oversight*[30]. Ritorneremo sul punto al termine di queste pagine.

Evgeny Morozov, uno dei più forti avversari del dataismo, ha sostenuto che l'ideologia del soluzionismo tecnologico che si riflette in queste visioni fallirà per due motivi[31]. In primo luogo, perché tratta le tecnologie come strumenti neutri per

19. Pagnanelli 2021.
20. Susca 2022.
21. Bennato 2022, p. 27 ss.
22. *Ivi*, p. 50.
23. Van Dijck 2014, p. 197 ss.
24. Harari 2015.
25. Lohr 2015.
26. Van Dijck 2014, p. 199 ss.
27. Han 2017.
28. Bennato 2022, pp. 50-51.
29. Purtroppo quell'articolo è poi soggetto a limiti sotto forma di eccezioni. Cfr. Simoncini 2021; Longo 2022; Falletti 2020.
30. Cfr. art. 14 del testo di compromesso diffuso il 3 febbraio 2024.
31. Morozov 2013, pp. 20-21.

produrre cose e risolvere problemi, piuttosto che come estensioni dei contesti di valore umano in cui operano. L'attivista sottolinea che fornire alle persone una nuova piattaforma non può risolvere i problemi della distorsione della realtà se le possibilità e i valori della piattaforma sono modellati dalle stesse condizioni politiche del problema. L'altro fallimento dell'ideologia del dataismo è il trattamento delle persone come nodi essenzialmente identici e intercambiabili in una rete di agenti razionali, piuttosto che come creature complesse, diverse e in costante sviluppo, quali siamo. L'ideologia sembra essere quella per cui se i tecnocrati si limitano a collegare tutti i nodi umani nel modo giusto e a far sì che i flussi di informazione tra di essi avvengano nelle direzioni corrette e alle velocità necessarie, il sistema informatico si auto-ottimizzerà magicamente per i valori rilevanti. Ma le persone non possono essere trattate come nodi identici in una rete, perché non tutti rispondiamo o scambiamo informazioni allo stesso modo o con le stesse capacità e, soprattutto, non tutti cerchiamo di ottimizzare lo stesso insieme di valori o di bilanciarli in egual modo.

Per le stesse ragioni sottolineate da Morozov, il già citato Han invece evidenzia che il nuovo totalitarismo dei dati non ha una ideologia, in quanto si fonda su «operazioni algoritmiche senza un'anima» che sono, appunto, "date"[32].

Il dataismo, con le sue conseguenze totalitarie e anti-ideologiche, ci aiuta a focalizzare un aspetto essenziale della realtà rappresentata dai dati. Questa non è gemella della realtà naturale ma gli somiglia, ne ha alcune proprietà e dettagli, nella misura in cui la tecnologia usata (gli algoritmi) e le risorse da questa impiegate (i dati) consentono di progettarne la somiglianza. È quindi una realtà isomorfa che però, in quanto rappresentazione della realtà reale, necessariamente ha un effetto distorsivo di quest'ultima (un po' come la relazione che si instaura tra una mappa e il territorio da questa rappresentato).

Questo fenomeno distorsivo influenza grandemente il diritto e le relazioni socio-economiche alle quali quest'ultimo presta i suoi strumenti tecnici. Prima però di scendere dentro all'analisi di alcuni degli aspetti del fenomeno giuridico facendoci guidare dall'esame dei saggi di questo speciale, vediamo alcune distorsioni prodotte dall'uso sociale degli algoritmi (gli strumenti informatici usati per la costruzione della società dei dati o anche la "mente" della società digitale).

4. Distorsioni

In un mondo datificato, il controllo degli algoritmi permette una costruzione e ricostruzione ibrida della realtà. Gli algoritmi garantiscono la manipolazione della società datificata e producono conseguenze distorsive sulla nostra rappresentazione del mondo sotto forma di dati[33].

Senza alcuna pretesa di esaustività, ma solo per introdurre al tema analizzato in questa sezione monografica, proviamo a individuare i principali effetti distorsivi che determina riflessivamente l'operare degli algoritmi sulla realtà datificata.

La prima distorsione concerne la progettazione degli algoritmi. Essi incorporano sia le teorie delle relazioni e del comportamento umano, sia gli obiettivi economici dei soggetti che li hanno progettati, sia ancora i possibili errori che gli esseri umani stessi possono aver compiuto nella stessa progettazione.

La seconda distorsione concerne le conseguenze derivanti dall'operare degli algoritmi. Essi, da un lato, producono una diversa percezione soggettiva del mondo per coloro che ne sono soggetti, soprattutto legata all'operare stesso delle tecnologie digitali e, dall'altro, grazie alle loro performance, determinano conseguenze implicite o collaterali, come il non riuscire a cogliere tutte le sottigliezze della realtà rappresentata o l'orientamento dei comportamenti delle persone.

Da questi due profili di distorsione o manipolazione derivano conseguenze di non poco momento per gli assetti sociali ma anche per le nostre esistenze. Ne sottolineiamo solo una: non è solo il mondo nel quale siamo immersi a essere diverso dal passato (anche recente) ma perfino noi stessi, la nostra soggettività e la nostra capacità di agire[34];

32. Han 2017, p. 10: «Quando si riuniscono (le persone), non formano una massa ma uno sciame digitale; non seguono un leader ma molti influencer».

33. Bennato 2022, p. 57.

34. O'Neil 2016; Cardon 2016.

una rivoluzione preoccupante per gli effetti che produce soprattutto nelle persone più giovani[35].

5. Cinque percorsi di analisi

L'esame fin qui condotto non può che a questo punto rivolgersi alla scoperta di ciò che abbiamo imparato leggendo i saggi di questo numero. Lo faremo mettendo in campo l'analisi di sei ambiti del diritto pubblico che, pur rimanendo sullo sfondo, a volte implicitamente e a volte esplicitamente, delle narrazioni svolte dagli autori, sono decisive per capire la colonizzazione del quotidiano da parte della tecnologia dei dati.

Il primo ambito toccato dai saggi è quello della "sicurezza". Con la società datificata si è incrinato il modello securitario moderno che era fondato sulla alterità soggettiva dello Stato nei confronti dei suoi cittadini. La tumultuosità con la quale si vanno assommando gli avanzamenti tecnologici attestano una ingovernabilità della nuova società con tecniche giuridiche elaborate tempi addietro. I processi tecnologici appaiono refrattari a una completa disciplina politico giuridica *ex-ante*[36]. Si delineano così, come ha messo ben in luce Federico Serini nel suo saggio[37], sistemi interstiziali di normazione securitaria legati a settori e questioni specifiche ove prevale il riferimento a forme diffuse di autoregolamentazione o di co-regolamentazione. Proliferano meccanismi privati, sistemi di certificazione il cui effetto non è solo la protezione di una "merce" ma della libertà stessa delle persone. È molto utile, quindi, quanto descrive Serini, perché ci fa vedere come la nostra libertà, sia negli spazi pubblici che privati, dipenda oggi da meccanismi privati securitari anziché solo da una dinamica di tipo pubblicistico[38].

Il secondo ambito interessato è quello della "giustizia". Il saggio di Irene Sigismondi[39] pone una questione capitale relativa al rischio di una privatizzazione della giustizia. Il tema delle *Online Dispute Resolutions* è oramai maturo e deve essere ben compreso se si vuole imprimere una svolta alla risoluzione delle controversie fuori dalle aule della giustizia tradizionale. La galassia di questi strumenti è amplissima e si fatica a volte a orientarsi al suo interno. Ciò che oggi abbiamo imparato è che l'evoluzione della società dei dati non sempre aiuta nella riduzione del contenzioso, ma anzi ne genera di nuovi. Va però sottolineato che le ODR nascono proprio nel momento in cui la rete Internet aveva ampliato il numero e le tipologie delle controversie sui prodotti scambiati attraverso il commercio elettronico, che aveva sì abbattuto i confini statali, ma aveva anche creato un nuovo tipo di contenzioso per risolvere il quale gli strumenti più risalenti non erano sempre adeguati[40].

Il terzo ambito toccato dai saggi concerne la "politica". Il saggio di Angela Cossiri[41] sottolinea i rischi più importanti che il processo di datificazione ha generato. Quei fenomeni di disinformazione e di cattiva formazione del mercato delle idee che determinano grandi incertezze per la vita democratica. Rispetto a questi problemi credo sia il caso di evidenziare un fenomeno che viene prima di tali distorsioni per capirne e segnalarne gli effetti. La datificazione è una forma neocoloniale di sfruttamento della ricchezza. Non intendo tornare al mantra di qualche anno fa per il quale i dati sono il "nuovo petrolio" ma anzi sottolineare come nella società dei dati, grazie ai dispositivi, chi si appropria della vita umana ha diritto alla estrazione di valore da essi. È una nuova forma di biopolitica, come ci indicherebbe Michel Foucault[42]. Invece di territori, risorse naturali e lavoro di schiavi, il colonialismo dei dati si appropria di corpi e risorse sociali. Sebbene le modalità, le intensità, le scale e i contesti del colonialismo dei dati siano diversi da quelli del colonialismo storico, la funzione rimane la stessa: espropriare la vita e le relazioni sociali delle persone della possibilità di essere completamente libere.

35. Calzolaio 2023a.
36. Bombelli 2017.
37. Serini 2023.
38. Iannuzzi-Laviola 2023.
39. Sigismondi 2023.
40. Sia consentito sul punto un rimando a Longo 2023, p. 209 ss.
41. Cossiri 2023.
42. Foucault 2004.

Questa forma di espropriazione (o forma propria di un nuovo capitalismo) impiega arsenali molto accattivanti, dall'intelligenza artificiale al riconoscimento facciale e ai nuovi modelli di commercio elettronico, dagli attacchi cibernetici alla produzione di chip, fino agli accordi internazionali che regolano l'attribuzione e lo sfruttamento della proprietà intellettuale. In tale senso, l'economia dei dati coincide con la politica dei dati.

Il quarto ambito concerne la "sostenibilità" di questa nuova economia. Lo ricorda molto bene il saggio di Elia Cremona[43] che, pur non limitandosi a questo tema ma coprendo il vasto orizzonte dei modelli economici legati all'uso e condivisione dei dati, arriva a individuare un nuovo orizzonte per la scienza pubblicistica. Nella argomentazione di Cremona digitalizzazione e sostenibilità ridisegnano i termini entro cui il capitalismo dei dati si legittima e incorpora alcune delle critiche alla sua attuale configurazione. La sfida che questo saggio descrive è decisiva. La sostenibilità, in tutte le sue declinazioni, si afferma parallelamente al crescere della consapevolezza dell'entropia prodotta dal nostro modello di sviluppo economico. Sebbene tale presa di coscienza sia conosciuta da molti anni, la questione è stata a lungo negata, e solo dopo gli anni Dieci ha finalmente trovato spazio nelle agende di governi e imprese. Il sogno implicito è che, grazie alla ricerca e all'innovazione tecnologica, sia possibile annullare gli effetti generati dal modello di sviluppo basato sui dati, senza toccare il circuito economico-politico che lo sostiene. Vedremo come nei prossimi anni in Europa, a partire dal "Data Governance" e il "Data Act", troveremo una possibile strada per realizzare tali obiettivi. Molto dipenderà dalla capacità della nuova governance europea del digitale di offrire una «effettiva protezione ai cittadini e alle imprese europee contro gli abusi del potere digitale e, al tempo stesso, di liberare le energie creative e imprenditoriali del vecchio continente verso la produzione di piattaforme alternative»[44].

Il quinto e ultimo ambito concerne il tema forse più complesso di tutti per uno studioso di diritto pubblico, la "sovranità". Intendiamo con questo ultimo concetto l'esercizio legittimo del potere. Il concetto di sovranità evoca una pletora di problemi, manifestazioni e immagini che si dipanano nella storia fino ai giorni nostri[45]. Oltre al controllo sull'economia, al potere di fare la guerra ed esercitare la forza legittima nei confronti dei consociati e all'esercizio della giustizia (moneta, spada, bilancia), il concetto di sovranità implica "diversi livelli di mediazione" (tra cittadino e sovrano, tra sovrano e i poteri derivati per l'esercizio della sovranità, tra unicità e pluralità di sovrani). Questo concetto trova oggi nuove forme di legittimazione come pure limiti nella società dei dati. Tanto che si parla di una "sovranità digitale" o sovranità sui dati, intesa come una forma di autorità legittima di controllo su dati, software, standard, servizi e infrastrutture digitali[46]. I termini sono sfuggenti, come d'altronde sottolinea molto acutamente Stefano Torregiani[47], che evidenzia quanto la nuova società metta in crisi la triade formata da territorio, sicurezza ed extraterritorialità. E allora si comprende l'obiettivo dell'Ue di rimuovere gli ostacoli alla libera circolazione di dati non personali tra differenti paesi Ue e tra i sistemi tecnologici ivi localizzati, permettendo alle imprese e alle pubbliche amministrazioni il trattamento e la conservazione dei dati ovunque vogliano all'interno dell'Unione. Il tema è delicato e coinvolge la fiducia nei trattamenti transfrontalieri di dati; infatti troppe volte si ricorre, come sottolinea Torregiani, alla localizzazione come uno strumento per garantire la sicurezza dei dati[48].

6. Il diritto costituzionale e la mutazione antropologica del XXI secolo: tre (meta)principi su cui scommettere

All'interno di questo quadro qui si apre un discorso sul quale saremo impegnati nei prossimi anni sui vantaggi e i rischi presenti nel nuovo mondo

43. Cremona 2023.
44. Santaniello 2021.
45. Mannoni-Stazi 2021.
46. Roberts-Cowls-Casolari 2021.
47. Torregiani 2023.
48. In questo senso v. anche Bassi 2022.

digitale[49]. Da qualche anno nell'Unione europea si è affacciata l'esigenza, sia a livello normativo che giurisprudenziale, di un quadro teorico costituzionale in grado di rileggere e riequilibrare il sistema dei poteri e delle libertà nella cornice di questo mondo che scienza e tecnica stanno sviluppando attraverso l'impiego di strumenti in cui la scienza dei dati e le intelligenze artificiali assumono un ruolo trasformativo come mai nessuna tecnologia lo aveva avuto[50].

Rispetto a questo scenario occorre un nuovo registro di lettura dei fatti – di cui però qui non ci occuperemo, in quanto ambito d'elezione dei filosofi[51] – e della necessità di poggiare su nuovi principi capaci di arricchire e correggere gli sviluppi della *datafication*.

A questo proposito si segnalano tre principi (nuovi) di natura (oramai) costituzionale che si vedono nascere nella realtà dell'impiego delle tecnologie digitali. Essi corrispondono a tre aspetti sottesi al discorso portato avanti da alcuni dei lavori qui pubblicati e che credo debbano arricchire il quadro dell'impegno europeo sul fronte dei valori costituzionali.

Il primo principio che segnaliamo è identificabile come il principio della "giustizia dei dati" o *data justice*. In questi anni i giuristi hanno discusso intensamente di protezione dei dati personali all'interno dell'orizzonte della rivoluzione tecnologica avvenuta con i *Big Data*[52]; meno attenzione è stata rivolta a un altro ambito di indagine connesso alla datificazione della vita che prende il nome di *data justice*[53]. Tale concetto – di origine sociologica – cerca di applicare i principi e le pratiche della giustizia sociale alle dinamiche sociali ed economiche che oggi sono guidate dal processo di datificazione. È quindi un'idea indeterminata ma che può divenire molto efficace se considerata nel quadro più vasto della semplice osservazione sociale, quale è quello della tutela dei diritti nello Stato costituzionale. Il punto di partenza assunto dalla *data justice* è che così come un'idea di giustizia serve per stabilire la *rule of law*, un'idea di "giustizia dei dati", intesa come equità e correttezza nel modo in cui le persone producono i dati, vengono rappresentate, classificate e trattate sulla base dei dati digitali, deve essere usata e rispettata in tutte le fasi politiche e tecniche del "governo" dei dati[54].

Si è già detto che la *datafication* è ampiamente considerata come un motore di efficienza e miglioramento nelle aree della scienza, del governo, delle imprese e della società civile. Queste trasformazioni presentano sfide sociali significative e richiedono di ricalibrare le garanzie delle libertà individuali e collettive.

A questo scopo la *data justice* emerge come un concetto chiave per affrontare tali sfide, privilegiando una preoccupazione esplicita per la giustizia sociale. Il concetto non è di per sé nuovo ma se viene utilizzato per aprire la strada a un cambiamento nella comprensione di ciò che è in gioco con la *datafication*, ben oltre la sfera del diritto alla protezione dei dati personali, può rappresentare un avanzamento considerevole. Ad esempio, un aspetto fondamentale che la *data justice* aiuta a mettere a fuoco è come bilanciare e integrare la necessità di essere rappresentati correttamente attraverso i dati con i bisogni che abbiamo di autonomia e integrità e con il principio di minimizzazione[55]; come pure attraverso di esso si può comprendere quali sono

49. Brownsword 2022.

50. Ellul 1969.

51. Floridi 2017.

52. Richards-King 2013.

53. Per una descrizione del concetto si vedano Dencik-Hintz-Cable 2016; Taylor 2017.

54. Taylor 2023.

55. Man mano che l'IA diventa sempre più una parte importante del potenziale ciclo di vita dei dati, per addestrare, parametrizzare e alimentare modelli di business e politiche, questa dinamica in cui i dati riflettono il potere esistente e i suoi interessi vengono amplificati. I dati ora non sono solo utili per rendere visibile il comportamento e il movimento delle popolazioni, sono utili per ottimizzarli. Perciò, qualsiasi mancanza di rappresentatività o comprensione degli interessi e delle dinamiche che i dati riflettono si traduce, grazie al passaggio dalla modellazione all'ottimizzazione, in una discriminazione diretta delle opportunità e delle possibilità dei soggetti. Dencik-Hintz-Redden-Treré 2019.

i principi di buona governance per l'uso dei *Big Data* in un contesto democratico e chi dovrebbe essere responsabile della loro determinazione.

Il secondo principio costituzionale che si affaccia nella nuova era datificata è la "trasparenza algoritmica" o *algorithmic transparency*. Di questo principio si è parlato moltissimo negli ultimi anni[56]. Se ne discute in termini tecnici quando ci si riferisce alla mancanza di trasparenza dovuta alla opacità innata e alla asimmetria algoritmica che caratterizza le macchine dotate di potere computazionale sui dati[57]; in questi termini anche i giudici amministrativi italiani hanno preso in considerazione la possibile coincidenza tra legalità e operazioni algoritmiche[58].

La trasparenza algoritmica viene in evidenza quando ci si riferisce al diritto a non essere sottoposti a forme di trattamento di dati completamente automatizzate senza che ciò implichi un diritto a conoscere in che modo le macchine abbiano elaborato quei dati[59], ma è venuto in evidenza anche in casi più delicati relativi alla protezione dei diritti fondamentali[60]. Tale principio implica veri e propri obblighi quando si discute delle garanzie che devono essere prestate dalle piattaforme per limitare gli effetti dovuti alla eccessiva concentrazione del potere nelle loro mani e alla moderazione dei contenuti diffusi[61]. Tra i valori da preservare durante gli impieghi delle tecnologie, la trasparenza algoritmica è quella più difficile da realizzare, ma è evidente che si tratta di un elemento essenziale del nuovo rapporto che abbiamo con le macchine e del modo in cui gli stessi pubblici poteri devono garantire l'uso pubblico di tali oggetti.

Il terzo principio di cui diamo qui sintetica indicazione – ma di cui già avevamo accennato *supra* – è il "controllo umano" o *human oversight*. Esistono diversi modelli di monitoraggio umano delle decisioni algoritmiche che, seppur con gradi e modi diversi, individuano strategie per assicurare che la decisione algoritmica sia sottoposta allo scrutinio di un essere umano. La supervisione umana aiuta a garantire che un sistema di intelligenza artificiale non comprometta l'autonomia umana o causi altri effetti negativi, come ad esempio i *bias*. Come ha avuto modo di indicare il "Gruppo di esperti della Commissione europea sull'IA" nel 2018, per avere una IA affidabile, etica e incentrata sull'uomo occorre garantire un adeguato coinvolgimento degli esseri umani nelle applicazioni di tali sistemi[62].

Le indicazioni del Gruppo di esperti sono arrivate fin nella proposta, già citata, di legge europea sull'IA (*AI Act*), dove all'articolo 14 si richiede la supervisione umana sui sistemi di IA "ad alto rischio" al fine di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali quando un tale tipo di IA è utilizzato conformemente alla sua destinazione o in condizioni di uso improprio ragionevolmente prevedibile.

Di questi tre principi sentiremo certamente parlare nei prossimi anni. Il "Codice dei contratti pubblici" (d.lgs. 31 marzo 2023, n. 36), ad esempio, indica, quali valori fondamentali nell'uso delle IA e della Blockchain nei contratti pubblici (art. 30), la "conoscibilità e comprensibilità", la "non esclusività della decisione algoritmica" e la "non discriminazione algoritmica"[63].

Queste sono solo alcune delle riflessioni che è possibile oggi svolgere tanto come analisi degli sviluppi della società datificata quanto come proiezione futura sulle grandi partite che l'uso delle

56. Simoncini 2019.

57. Busuioc-Curtin-Almada 2022.

58. Sul tema si vedano *infra multis* Simoncini 2020; Gallone 2023.

59. Malgieri 2022.

60. Si vedano a tal proposito le tutele che sono state individuate in un caso recente avvenuto in Galles relativo al riconoscimento facciale massivo in luoghi pubblici, sul quale si veda Pin 2019. In generale sul tema si veda Mobilio 2021.

61. Si veda a tale proposito il regolamento (UE) 2022/2065 "relativo al mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE" noto anche come *Digital Services Act* (DSA). Sul tema sia consentito rimandare a Longo 2023a.

62. High-Level Expert Group on Artificial Intelligence 2019.

63. Zicaro 2023.

intelligenze artificiali stanno aprendo sul piano costituzionale in una competizione che è ormai di carattere mondiale, ma dove l'Europa, utilizzando sia il peso di un apparato di governo molto solido sia le tradizioni costituzionali comuni ai paesi dell'Unione, ha molto da difendere e da affermare.

Riferimenti bibliografici

D. Acemoglu, S. Johnson (2023), *Potere e progresso. La nostra lotta millenaria per la tecnologia e la prosperità*, il Saggiatore, 2023

C. Anderson (2008), *The End Of Theory: The Data Deluge Makes The Scientific Method Obsolete*, in "Wired", 23 June 2008

V. Bakir, A. Laffer, A. McStay (2023), *Blurring the Moral Limits of Data Markets: Biometrics, Emotion and Data Dividends*, in "AI & SOCIETY", 25 July 2023

G. Balbi (2022), *L'ultima ideologia. Breve storia della rivoluzione digitale*, Laterza, 2022

L. Barra, L. Sartori (2022), *L'infrastruttura che permea le nostre vite*, in "il Mulino", 2022, n. 3

E. Bassi (2022), *Dati, sovranità, nuovi modelli di governance*, in U. Pagallo, M. Durante (a cura di), "La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società", Mimesis, 2022

D. Bennato (2022), *La società del XXI secolo. Persone, dati, tecnologie*, Laterza, 2022

G. Bombelli (2017), *Dal moderno all'"ultramoderno"? Intorno al nesso diritto-tecnica-sicurezza*, in F. Pizzolato, P. Costa (a cura di), "Sicurezza e tecnologia", Giuffrè, 2017

R. Brownsword (2022), *Rethinking Law, Regulation, and Technology*, Edward Elgar, 2022

M. Busuioc, D. Curtin, M. Almada (2022), *Reclaiming transparency: contesting the logics of secrecy within the AI Act*, in "European Law Open", 2022, n. 1

S. Calzolaio (2023), *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale. Introduzione*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2023a), *Social media e minori. Il Safety-first approach*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2017), *Protezione dei dati personali*, in "Digesto delle discipline pubblicistiche", Aggiornamento, UTET, 2017

D. Cardon (2016), *À quoi rêvent les algorithmes? Nos vies à l'heure des big data*, Éditions du Seuil et La République des Idées, trad. it. *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Mondadori, 2016

M. Castells (2019), *Foreword*, in M. Graham, W.H. Dutton (eds.), "Society and the internet: How networks of information and communication are changing our lives", II ed., Oxford University Press, 2019

M. Castells (2006), *Galassia internet*, Feltrinelli, 2006

A.C. Clarke (1962), *Profiles of the Future: An Inquiry into the Limits of the Possible*, I ed., Harper & Row, 1962

A. Cossiri (2023), *Le campagne di disinformazione nell'arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento,* in "Rivista italiana di informatica e diritto", 2023, n. 2

E. Cremona (2023), *Quando i dati diventano beni comuni: modelli di* data sharing *e prospettive di riuso,* in "Rivista italiana di informatica e diritto", 2023, n. 2

L. Dencik, A. Hintz, J. Redden, E. Treré (2019), *Exploring Data Justice: Conceptions, Applications and Directions*, in "Information, Communication & Society", 2019, n. 7

L. Dencik, A. Hintz, J. Cable (2016), *Towards data justice? The ambiguity of anti-surveillance resistance in political activism*, in "Big Data & Society", 2016, n. 2

J. Ellul (1969), *La tecnica rischio del secolo*, Giuffrè, 1969

E. Falletti (2020), *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in "Il diritto dell'informazione e dell'informatica", 2020, n. 2

L. Floridi (2017), *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Raffaello Cortina, 2017

C. Formenti (2010), *Sfera pubblica e nuovi media*, in "Politica del diritto", 2010, n. 3

M. Foucault (2004), N*aissance de la biopolitique. Cours au Collège de France 1978-1979*, Seuil/Gallimard, 2004, trad. it. *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, Feltrinelli, 2005

G. Gallone (2023), *Riserva di umanità e funzioni amministrative*, CEDAM - Wolters Kluwer, 2023

A. Gatti (2019), *Istituzioni e anarchia nella Rete. I paradigmi tradizionali della sovranità alla prova di Internet*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 3

C. Giaccardi, M. Magatti (2022), *Supersocietà: ha ancora senso scommettere sulla libertà?*, il Mulino, 2022

B.-C. Han (2017), *Psychopolitics: Neoliberalism and New Technologies of Power*, Verso, 2017

Y.N. Harari (2015), *Homo Deus: A brief history of tomorrow*, Random House, 2015

High-Level Expert Group on Artificial Intelligence (2019), *Ethics Guidelines for Trustworthy AI*, Brussels, 8 April 2019

A. Iannuzzi, F. Laviola (2023), *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in "Diritto costituzionale", 2023, n. 1

S. Lohr (2015), *Data-ism: Inside the big data revolution*, Simon and Schuster, 2015

E. Longo (2023), *Giustizia digitale e Costituzione: riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Franco Angeli, 2023

E. Longo (2023a), *Libertà di informazione e lotta alla disinformazione nel Digital Services Act*, in "Giornale di diritto amministrativo", 2023, n. 6

E. Longo (2022), *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione", vol. I, il Mulino, 2022

E. Longo (2019), *Dai big data alle «bolle filtro»: nuovi rischi per i sistemi democratici*, in "Percorsi costituzionali", 2019, n. 1

M. Lycett (2013), *'Datafication': Making sense of (big) data in a complex world*, in "European Journal of Information Systems", 2013, n. 4

G. Malgieri (2022), *Automated Decision-making and Data Protection in Europe*, in G. González Fuster, (ed.), "Research Handbook on Privacy and Data Protection Law", Edward Elgar Publishing, 2022

S. Mannoni, G. Stazi (2021), *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Editoriale Scientifica, 2021

V. Mayer-Schönberger, K. Cukier (2013), *Big Data: A Revolution that Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, 2013

G. Mobilio (2021), *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021

E. Morozov (2013), *To Save Everything, Click Here: The Folly of Technological Solutionism*, PublicAffairs, 2013

C. O'Neil (2016), *Weapons of Math Destruction*, Penguin Books, 2016, trad. it. *Armi di distruzione matematica*, Bompiani, 2017

V. Pagnanelli (2021), *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in "Rivista italiana di informatica e diritto", 2021, n. 1

J. Pearl, D. Mackenzie (2018), *The Book of Why*, Basic Books, 2018

A. Pin (2019), *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in "DPCE online", 2019, n. 4

N.M. Richards, J.H. King (2013), *Three paradoxes of big data*, in "Stanford Law Review", vol. 66, 2013, n. 1

H. Roberts, J. Cowls, F. Casolari et al. (2021), *Safeguarding European values with digital sovereignty: An analysis of statements and policies*, in "Internet Policy Review", 2021, n. 3

M. Santaniello (2021), *La regolazione delle piattaforme e il principio della sovranità digitale*, in "Rivista di Digital Politics", 2021, n. 3

F. Serini (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2

I. Sigismondi (2023), *Piattaforme di risoluzione alternativa delle controversie online tra frammentazione di Internet e istanze di giustizia*, in "Rivista italiana di informatica e diritto", 2023, n. 2

A. Simoncini (2021), *Art. 22*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

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

A. Simoncini (2020a), *Il diritto alla tecnologia e le nuove diseguaglianze*, in F.S. Marini, G. Scaccia (a cura di), "Emergenza Covid-19 e ordinamento costituzionale", Giappichelli, 2020

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

V. Susca (2022), *Tecnomagia: estasi, totem e incantesimi nella cultura digitale*, Mimesis, 2022

L. Taylor (2023), *Data justice, computational social science and policy*, in E. Bertoni, M. Fontana, L. Gabrielli et al. (eds.), "Handbook of computational social science for policy", Springer, 2023

L. Taylor (2017), *What is data justice? The case for connecting digital rights and freedoms globally*, in "Big Data & Society", 2017

S. Torregiani (2023), *Il* Data Act*: una versione europea del* Data Nationalism*?*, in "Rivista italiana di informatica e diritto", 2023, n. 2

J. Van Dijck (2014), *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in "Surveillance & society", vol. 12, 2014, n. 2

A.A. Wallace (2021), *Social Media for Social Good Through a Public Policy Lens: What Role Does Social Media Play in the Creation and Sustainability of Social Movements?*, in R. Luttrell, L. Xiao, J. Glass (eds.), "Democracy in the disinformation age: Influence and activism in American politics", Routledge, 2021

V. Zicaro (2023), *La digitalizzazione*, in G.F. Cartei, D. Iaria (a cura di), "Commentario al nuovo Codice dei contratti pubblici", Editoriale Scientifica, 2023

S. Zuboff (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019

Studi e ricerche

Note e discussioni

Osservatori

Recensioni

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0118 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Antonio José Sánchez Sáez

El posible uso de la inteligencia artificial en el ámbito judicial: contexto jurídico español y europeo. Especial referencia al contencioso-administrativo

En esta investigación hemos querido indagar en las posibilidades que tienen los sistemas de inteligencia artificial de ser utilizados en el ámbito judicial en España, aunque bien podríamos extrapolar nuestras conclusiones a cualquier otro Estado de Derecho europeo. Sabemos que en Estados Unidos y en el mundo anglosajón en general el uso de estos sistemas está prácticamente liberalizado, pero el proyecto de Reglamento sobre IA de la Unión Europea y el proyecto de Convenio Marco sobre IA del Consejo de Europa imponen límites a la proporcionalidad y el respeto de los derechos fundamentales que son ciertamente necesarios para no socavar las garantías procesales. Los órdenes jurisdiccionales más adecuados para el uso de la IA son el penal y el civil, ya que el contencioso-administrativo, con sus potestades discrecionales, sus conceptos jurídicos indeterminados y la existencia de intereses generales lo hacen inadecuado. Sin embargo, hemos propuesto algunos usos posibles en este proceso.

Inteligencia artificial – Algoritmos – Proceso – Administración de justicia – Contencioso-administrativo

The use of artificial intelligence in the judicial field: the Spanish and European legal context. Special reference to contentious-administrative Courts

In this research we want to investigate the possibilities that artificial intelligence systems have of being used in the judicial field in Spain, although we could well extrapolate our conclusions to any other European Rule of Law. We know that in the United States and in the English-speaking world in general the use of these systems is practically liberalized, but the draft Regulation on AI of the European Union and the draft Framework Convention on AI of the Council of Europe impose limits on proportionality and respect for fundamental rights which are certainly necessary in order not to undermine procedural guarantees. The most appropriate jurisdictional orders for the use of AI are criminal and civil, since contentious-administrative, with its discretionary powers, its indeterminate legal concepts and the existence of general interests make it inappropriate. However, we have proposed some possible uses in this process.

Artificial intelligence – Algorithms – Process – Administration of justice – Contentious-administrative

El Autor es catedrático de Derecho administrativo - Universidad de Sevilla

1. Introducción. Las limitaciones de la IA en el mundo del derecho

Ser juzgado por un hombre justo e imparcial es una exigencia mínima de civilización y garantía de paz y de orden social. El juez es persona y, como tal, no le son ajenas las pasiones humanas que subyacen en los conflictos que tiene que resolver. El juez intenta discernir lo correcto de lo incorrecto y solucionar las disputas conforme al Derecho que conoce. Esa justicia humana, aunque imperfecta, la ejercen los jueces de forma vicarial, en nombre del Rey, emanando del pueblo (art. 117 de la Constitución española, CE).

La esencia de la labor judicial es conocer las pretensiones de las partes, otorgar o no una justicia cautelar, comprobar la veracidad de las pruebas y, finalmente, resolver el pleito. Esa labor, en última instancia, merece siempre una "reserva de humanidad[1]" (o principio de inclusión), que no debe ser nunca reemplazada por la máquina, ni verse comprometida por ella.

Así las cosas, defenderemos en esta investigación que los sistemas de inteligencia artificial pueden y deben ayudar al Juez a tomar esas decisiones mejor, con mayor celeridad, eficacia y eficiencia, pero debiendo quedar siempre circunscritas a esa labor subalterna, adjetiva y asistencial, nunca sustancial. Incluso podría darse el caso de que algún *chatbox* pudiera ayudar al juez a elaborar el borrador de una sentencia de poca cuantía o un juicio monitorio, pero debiendo existir siempre la opción del juez de adoptarla o rechazarla o modificarla.

No existe una definición concreta de IA[2]. A nivel jurídico, desde luego incluye los sistemas que más usamos los jueces y el resto de operadores

1. No se puede ocupar el lugar de un ser humano a la hora de dictar sentencia o tomar decisiones (Resolución del Parlamento Europeo de 20 de enero de 2021, *Inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho Internacional*).
2. El Dictamen sobre Inteligencia artificial del Comité Económico y Social europeo, de 31 de mayo y 1 de junio de 2017 concluye que «No existe una definición establecida y unánimemente aceptada de la IA. La IA es un concepto que engloba muchas otras (sub)áreas como la informática cognitiva (*cognitive computing*: algoritmos capaces de razonamiento y comprensión de nivel superior – humano –), el aprendizaje automático (*machine learning*: algoritmos capaces de enseñarse a sí mismos tareas), la inteligencia aumentada (*augmented intelligence*: colaboración entre humanos y máquinas) o la robótica con IA (IA integrada en robots). Sin embargo, el objetivo fundamental de la investigación y el desarrollo en materia de IA es la automatización de compor-

jurídicos: los repertorios legislativos o bases de datos informatizadas de doctrina, jurisprudencia y doctrina legal (sistemas expertos), que nos ayudan a escrutar y organizar razonadamente los datos, siendo imprescindibles desde hace ya años para elaborar una investigación jurídica o, en el caso de funcionarios y otros jueces, como fundamento de actos administrativos o de sentencias, respectivamente. Pero va más allá.

Porque estamos hablando ya de la existencia de algunas herramientas que pueden trascender el rol de "ayuda" para decidir cuestiones de fondo o que lo afecten de manera directa, como el estudio de la probabilidad de reincidencia de un preso, la posibilidad de ganar o perder un pleito en atención al juez que ha de resolver el caso, al abogado que nos defiende o al asunto mismo, la existencia de pruebas mediante reconocimiento biométrico a distancia[3], la redacción misma de la sentencia, el otorgamiento o no de medidas cautelares, la probabilidad de ataques de violencia doméstica[4], etc. No se trata de que la IA use un método distinto al de las aplicaciones y repertorios que solemos usar los juristas (el método se basa en tratamiento masivo de datos mediante algoritmos) sino que su capacidad y complejidad es tal que pueden llegar a construir razonamientos jurídicos completos, que puede usar el juez para resolver partes esenciales del proceso.

Es importante partir de un hecho incontrovertible: la expresión "inteligencia artificial" es un oxímoron, porque realmente ninguna máquina tiene conciencia de sí misma ni capacidad de ser realmente inteligente en el sentido humano; no basta con organizar y recopilar muchos datos; no basta con generar un resultado cribado y aparentemente

tamientos inteligentes como razonar, recabar información, planificar, aprender, comunicar, manipular, observar e incluso crear, soñar y percibir» (Dictamen del Comité Económico y Social Europeo sobre la Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad).

3. Sin embargo, el PP europeo está presionando para que se permita el reconocimiento facial por razones de seguridad, expresando durante los últimos meses la necesidad de que la normativa garantice la posibilidad de recurrir a herramientas de reconocimiento facial, tanto en tiempo real como en grabaciones, en la lucha contra el terrorismo y en la búsqueda de personas desaparecidas, especialmente en el caso de menores: «Es crucial garantizar la seguridad. Por eso esta legislación debe contar con instrumentos eficientes para, por ejemplo, prevenir atentados terroristas, buscar personas desaparecidas y, en especial, poder actuar en todo aquello que afecte a la vida de los niños. En todos estos casos debe haber una autorización judicial y una definición temporal de aplicación», apuntó ayer la eurodiputada del PP Pilar del Castillo." Fuente: https://www.abc.es/tecnologia/informatica/soluciones/ue-aprueba-ley-controlar-peligros-inteligencia-artificial-20230614141019-nt.html. Corremos, además, el riesgo, de usar los sistemas de vigilancia masiva y sistemas de reconocimiento facial (SRF) como mecanismo invasivo de control poblacional, como se ha demostrado con el COVID hace pocos meses, señala Villegas Delgado 2023, p. 116. Esto, ciertamente, es peligroso pues sería abrir la Caja de Pandora a casos puntuales para luego imponer una seguridad férrea al estilo del partico comunista chino, atentando contra todos los derechos de la persona. Un cierto grado de inseguridad es tolerable si con ello logramos proteger el derecho a la intimidad, a la privacidad y a la protección de los datos personales de la persona en zonas públicas. En el fondo el usuario-administrado tiene un grave deber de ejercer su derecho a la "autodeterminación informativa", es decir, de controlar la información que vierte en Internet. La expresión procede del TC Federal alemán, en Sentencia de 15 de diciembre de 1983, sobre la Ley del Censo de 31 de marzo de 1982. Cfr. Murillo de la Cueva 2003, p. 39.

4. Un uso estándar del cálculo de probabilidades de violencia doméstica conforme a los datos introducidos puede dar un porcentaje de riesgo bajo, por falta de datos que hubieran arrojado un resultado más afinado, con un riesgo alto o muy alto. Fue el caso en el que una mujer fue asesinada por su pareja, pues la policía no protegió adecuadamente a la víctima al clasificar su caso como de riesgo bajo, por faltar datos del país de origen del asesino, que revelaban que era un maltratador ya desde entonces. La Audiencia Nacional condenó al Estado a pagar por responsabilidad patrimonial de la Administración, en 2020. Cfr. Abadías Selma 2022, p. 85. Fue la SAN (Sala 3ª, Sección 5ª) de 30 septiembre de 2020 (JUR 2020\290359), ponente Dña. María Luisa Sánchez Cordero.

orgánico, de carácter generativo, como hace Chatgpt y otros modelos fundacionales[5]; no basta tampoco con que las apps de despachos de abogados permitan ver la viabilidad de un caso; tampoco con la capacidad de aprendizaje de ciertos *bots*, ni de su capacidad de planear o dar líneas de solución de problemas complejos; tampoco sería suficiente para llamar inteligente a una máquina que ésta tenga capacidad de reconocer el entorno y de tomar decisiones, porque éstas derivan siempre de datos, de información, nunca de intuiciones o de elementos no sensibles. Por ejemplo, si a la máquina le faltan datos del entorno familiar de una persona, nunca podría proponer que un padre/madre con hijos menores salga en libertad bajo fianza para cuidar de ellos y no se quede en prisión preventiva, al margen de su porcentaje de reincidencia, obtenido mediante IA[6], algo que el Juez puede conocer por una simple pregunta.

Esto sea dicho para que rechacemos un enfoque "místico" de la IA, como un instrumento con capacidades mentales propias, que no tiene. Esta limitación intrínseca de la máquina, que no le permite ser inteligente por mucha potencia de tratamiento datos y de cálculo que tenga, se echa de ver en la definición que da el proyecto de Reglamento del Parlamento europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión en su art. 3.1[7], donde, a pesar de su esfuerzo por definir la IA como algo inteligente se ven las costuras del instrumento: se habla en concreto de IA generativa, pero sólo puede generar información; de diversos niveles de autonomía, pero nunca de autonomía plena, claro está; y de influencia en entornos reales o virtuales, pero nunca de capacidad de decisión propia. De hecho, no se nos ocurre una actividad intelectualmente más compleja que el juicio de un juez o magistrado, donde entran en juego elementos jurídicos y fácticos cuya interacción se escapa de la capacidad decisional de las máquinas. Siempre va a faltar en la IA el elemento de la autoconciencia, el elemento cognitivo, el intelectual y el volitivo, la comprensión de lo que se está leyendo y el razonamiento práctico.

En suma, las cualidades del cerebro humano y las potencias del alma estarán siempre fuera del alcance de cualquier máquina. Porque la inteligencia humana supone siempre un *plus*: la capacidad de ir más allá de los datos y de sus consecuencias lógicas. Por ejemplo, y aplicado al mundo del Derecho, la capacidad para inducir reglas no lógicas, es decir, consideraciones más allá de lo aparente[8], para establecer excepciones, para usar analogías o razonamientos parecidos, para discriminar datos o realzar otros aparentemente iguales, para captar la esencia de un problema jurídico, para saber evitar argumentos que pueden darle pistas a la otra parte, para darle la vuelta al razonamiento de la otra parte, para establecer argumentos filosóficos a mayor abundancia, *contrario sensu*, usar argumentos de autoridad, recurrir a principios jurídicos

5. Cfr. Barrio Andrés 2023. Aunque la versión de pago ya puede realizar investigaciones jurídicas, generar conocimientos, transformar textos, gestionar casos, revisar documentos, etc., no comprende lo que dice, tiene una experiencia limitada (no tiene el nivel de conocimiento jurídicos de un jurista avezado) y usa datos no actualizados (hasta septiembre de 2021). En el Reglamento IA de la UE los sistemas fundacionales se pueden integrar en sistemas de alto riesgo.

6. Cfr. Martínez 2017, p. 154, considera que la inteligencia intuitiva o emocional, propia de los seres humanos, y las decisiones derivadas de ella no son irracionales sino que difieren en muchas ocasiones de las resoluciones que propone la IA, que es incapaz de percibirlas, pues se atiene a la "dictadura de los datos".

7. «Sistema de inteligencia artificial (sistema de IA) es un sistema basado en máquinas, diseñado para funcionar con diversos niveles de autonomía y capaz, para objetivos explícitos o implícitos, de generar información de salida – como predicciones, recomendaciones o decisiones – que influya en entornos reales o virtuales». Esta nueva definición, más concreta, ha sido dada por el Parlamento, tras una enmienda aceptada (la 165) y aprobada por el mismo en su sesión de 14 de junio de 2023.

8. El *data mining*, propio de algunas IA, consiste en encontrar patrones lógicos interesantes a partir de mucha cantidad de datos: como se ve, las máquinas pueden inducir reglas y patrones, pero siempre de forma lógica, derivada de repeticiones. El hombre, en cambio, puede fijarse en elementos excepcionales no recurrentes o en elementos no sensibles a las máquinas.

no escritos, utilizar las palabras adecuadas… y, en general, a usar los miles de matices que sólo el juez humano conoce por ser hombre, para intentar alcanzar el ideal de la Justicia o, incluso, de apartarse de él deliberadamente y de manera sofística para defender una determinada posición jurídica. En definitiva, creo que la inteligencia humana nos permite entender la esencia de las cosas, la verdad objetiva de las mismas[9], yendo más allá de lo que aparentan ser, es decir, de lo sensible, del dato, de la información objetiva que tenemos de ellas, hasta entender lo que son realmente. De hecho, cuando un juez o un órgano administrativo resuelven un recurso estudian el caso a fondo, con todas sus características, y la legislación, jurisprudencia y doctrina aplicables[10]. Y cuando ha entendido el problema de fondo y el Derecho a aplicar *intelige* la que sería solución más justa al asunto, conforme a su pericia y la argumenta. Este modo de razonar no suele ser el de las máquinas, que llegan a soluciones necesarias e inexorables como consecuencias de silogismos, que pueden no llevar a resultados justos.

Dicho lo cual, es evidente que la IA tiene su papel en la actividad administrativa (análisis de datos, resolución de conflictos de poca importancia, resumen de información, ayuda en la prestación de servicios, lectura de textos, traducción a otros idiomas, etc.) y también en la administración de justicia, con aplicaciones, *bots* y herramientas que son cada vez mejores en el procesamiento de datos complejos que, bien utilizados, prestan un buen auxilio a los jueces y secretarios judiciales pero que, por culpa de los sesgos de los algoritmos y de un mal empleo (por falta de control humano) pueden llegar a influir negativamente en la imparcialidad y garantías del proceso judicial.

En resumidas cuentas, la IA es un instrumento en mano humana, al igual que un cuchillo o un martillo: éstos son fabricados por el hombre, igual que los sistemas de inteligencia artificial son diseñados por humanos, y ambos son instrumentos ciegos, que no piensan por sí mismos, ya que sólo hacen lo que el operador quiere que haga[11]. Podemos decir, pues, que los sistemas de IA son esclavos de su propio algoritmo y eso les impide pensar libremente, yendo más allá del mismo. No pueden hacer nada que su algoritmo no les permita, ni dejar de hacer nada que su algoritmo no les prohíba. Incluso cuando se nos presentan herramientas de IA fuertes que aprenden por sí mismas no es del todo cierto, pues se limitan a entresacar de los datos que las alimentan los más importantes o repetidos (*data mining*, en busca de patrones que se repiten), pero sin poder aportar nada por sí mismos. En el mundo del Derecho hay que evitar, por tanto, el determinismo de la máquina, exigiendo que la aplicación de la respuesta algorítmica siempre sea supervisada por el juez o magistrado.

9. El pensamiento (y, por ende, la argumentación jurídica) no es sólo una cuestión cerebral sino también del alma, que los cristianos creemos que forma parte esencial del ser humano, y que lo separa de otros animales. No por casualidad Platón (y luego San Agustín) decía que el pensamiento «es un diálogo del alma consigo misma». Y por eso una herramienta artificial nunca podrá pasar de acumular datos y de ofrecer patrones.

10. Aunque el sistema público de jurisprudencia CENDOJ, del CGPJ, ha mejorado en los últimos años, aún está lejos de los sistemas privados de pago como Aranzadi. En opinión de Martínez Gutiérrez 2019 el CGPJ debería realizar una compra pública para hacerse con los mejores sistemas de IA del mercado, que mejorase la eficacia y eficiencia de la labor jurisdiccional en España.

11. Todos los algoritmos, por tanto, tienen sesgos: los que incluyen en ellos sus diseñadores o las empresas que pagan a éstos para que se los diseñen. Como esas desviaciones siempre van a existir, el derecho a acceder a ellos es esencial en materia judicial, tanto por parte de los jueces como de los administrados. Y las revisiones por parte de organismos independientes. Los ingenieros informáticos tienen que ser conscientes del poder enorme que tienen, y de la ética de no vender su talento a empresas que pagan mucho para incluir sus sesgos e influir en asuntos públicos de especial trascendencia. Cfr. Asamblea Parlamentaria del Consejo de Europa, Recomendación n° 2102, de 28 de abril de 2017, Technological convergence, artificial intelligence and human rights: «Las referencias a la toma de decisiones independiente por parte de los sistemas de IA no pueden eximir a los creadores, propietarios y gerentes de estos sistemas de la responsabilidad por violaciones de los derechos humanos cometidas con estos sistemas, incluso en casos en que un acto responsable no haya sido ordenado directamente por un humano responsable comandante u operador. (140, n° 9. 1.1)».

Otro problema inherente a la IA, respecto a un cuchillo o un martillo, es que mientras que éstos son lo que vemos y no esconden nada, la IA puede contener sesgos de diseño que pueden dar resultados desviados, no conocidos por el juez. Ahí estriba su peligro, que se amplifica en un servicio público tan sensible como es la administración de justicia y, en particular, el contencioso-administrativo, donde existen intereses de carácter general en juego.

En relación con el proceso, suscribimos las palabras de Vallespín Pérez, cuando considera que debemos tener cuidado de no caer en un escenario de "dictadura digital", en el que las máquinas de IA sustituyan a los jueces humanos. En realidad, como dice Nieva Fenoll, estaríamos pasando de la justicia de los jueces a la justicia de los programadores y de aquéllos que les influyan[12]. Es mejor buscar un equilibrio entre la eficiencia procesal y el respeto de las garantías procesales básicas[13].

2. Los algoritmos y sus sesgos

Los algoritmos son ecuaciones matemáticas que se entrelazan para proporcionar un resultado, derivado del manejo de los *big data*, es decir, de grandes cantidades de datos previamente proporcionados[14]. Esos datos están previamente ordenados (*smart data*), como ocurre con las sentencias de una base de datos, o con la producción científica de la doctrina española, en herramientas recopilatorias de la misma. Esto, en el ámbito judicial, requiere un trabajo previo de automatización, para unificar los textos y hacerlos legibles y gestionables por el software de la IA (normalmente mediante su conversión a archivos pdf leíbles), como pretende la actual Estrategia Justicia 2030 del Estado español, de forma que los integrantes de la oficina judicial estarán obligados al uso integral de las aplicaciones informáticas, y el sistema de gestión procesal de esas aplicaciones[15]. A partir de esta automatización trabaja la IA.

En la UE se ha acuñado el principio *digital by default*, es decir, se prefiere la gestión y tramitación digital a igualdad de garantías administrativas. Pero este principio tiene, por su propia formulación, un anverso: se prefiere la tramitación en papel o con la presencia de personas si ello ofrece más garantías para las partes[16].

Los algoritmos son creaciones humanas, y, por lo tanto, heredan los sesgos y opiniones de los que los diseñan, ya sean empresas, Administraciones o informáticos autónomos, de forma que es inherente al algoritmo tener sesgos, es decir, una "opinión incrustada en las matemáticas"[17]. Cathy O'Neil, una altísima experta en algoritmos, graduada en matemáticas por Harvard, programadora informática y creadora de software y algoritmos, después de décadas trabajando en el sector, ha quedado tan desencantada que ha escrito un asperísimo libro titulado "Armas de destrucción matemática (ADM)", traducido al castellano y publicado en

12. Cfr. Nieva Fenoll 2022, p. 20.
13. Cfr. Vallespín Pérez 2023, p. 10.
14. Cfr. Pérez Estrada 2022, p. 32.
15. El Protocolo Marco de Actuación de la Oficina judicial, julio 2014, versión 3.0, emitido por la Secretaría general de la Administración de Justicia, Ministerio de Justicia, lo llama "tramitación judicial guiada", que supone el uso del mismo sistema de aplicaciones informáticas, cuya responsabilidad recae sobre los directores de los servicios comunes procesales y los secretarios judiciales. El art. 41.1 de la Ley 40/2015, de 1 de octubre, del Sector Público, lo llama "actuación administrativa automatizada", que es la realizada íntegramente a través de medios electrónicos, sin intervención de empleado público. Así, ocurre con los actos administrativos reglados y con ciertos actos como las multas de tráfico por radar (la máquina gradúa la multa según la velocidad del vehículo y la velocidad máxima permitida). Cfr. Martínez Gutiérrez 2019, p. 235.
16. Se trata de la "versión digital por defecto": las Administraciones públicas deberían prestar sus servicios en forma digital (incluida la información legible por máquina) como opción preferida (dejando otros canales abiertos para quienes estén desconectados por elección o necesidad). Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Plan de Acción sobre Administración Electrónica de la UE 2016-2020. Acelerar la transformación digital de la administración, Bruselas, 19.4.2016, COM (2016) 179 final.
17. Cfr. O'Neil 2017, p. 20.

España en 2017. Hace una durísima crítica a los programadores de algoritmos por los sesgos que deslizan en ellos, por la importancia que los políticos les atribuyen y, finalmente, por los daños que irrogan a los derechos fundamentales y a las personas, especialmente a las más débiles e iletradas[18].

Pero volvamos a la teoría. En ese manejo de datos, una vez preguntada la IA por una persona usuaria, a igualdad de datos, el algoritmo siempre va a arrojar el mismo resultado, de manera determinista. Podríamos decir que la ley interna de la IA son los algoritmos, normalmente opacos a los usuarios. Y éste es su principal problema, porque, aunque el futuro Reglamento sobre IA de la UE obligue a los programadores de IA a darlos a conocer o a explicar con palabras sencillas las reglas que juegan en cada uno de ellos para dar determinados resultados, es muy fácil que el gran público no se interese por ello (¿alguien lee las instrucciones de Google o Facebook o de las cientos de aplicaciones que tenemos instaladas en el móvil, antes de inscribirse o de descargárselas, presas como somos todos de esa especie de "furor informático" que nos invade? Incluso es muy posible que el fabricante o programador oculte el sesgo o parte de la información esencial de dicho algoritmo, por razones de celo ante su propiedad intelectual y para evitar la competencia desleal de otros *stakeholders*; o porque realmente no quieran dar a conocer el sesgo ideológico que le dan a sus algoritmos, para influir en los resultados de manera oculta[19].

Ciertamente, es muy loable que la UE esté a punto de aprobar un Reglamento de IA, conforme al principio de precaución, pero es dudoso que en este caso pueda darse el famoso "efecto Bruselas", como lo bautizó Anu Bradford (de emulación de

18. Copio un párrafo devastador, que puede bien ser el resumen de todo el libro: «En el año 2010 aproximadamente las matemáticas se habían impuesto como nunca antes en los asuntos humanos, y el público en general recibió el cambio con los brazos abiertos. Y, sin embargo, yo veía problemas en el horizonte. Estas aplicaciones fundamentadas en las matemáticas que alimentaba la economía de los datos se basaban en decisiones tomadas por seres humanos que no eran infalibles. Seguro que algunas de esas decisiones se tomaban con la mejor de las intenciones, pero muchos de estos modelos programaban los prejuicios, las equivocaciones y los sesgos humanos en unos sistemas informáticos que dirigían cada vez más nuestras vidas. Cuales dioses, estos modelos matemáticos eran opacos y sus mecanismos resultaban invisibles para todos, salvo para los sumos sacerdotes del sector: los matemáticos y los ingenieros informáticos. Sus veredictos, incluso cuando estaban equivocados o eran perjudiciales, eran indiscutibles e inapelables y solían castigar a los pobres y los oprimidos de nuestra sociedad, al tiempo que enriquecían a los ricos. Se me ocurrió un nombre para este tipo de modelos perniciosos: armas de destrucción matemática (ADM)». Cfr. O'Neil 2017, p. 11.

19. Sevilla ha sido elegida como sede europea del Centro Europeo de Transparencia algorítmica (ECTA) y sus primeros profesionales ya están trabajando, a la espera de que se construya el nuevo edificio. Este centro se deriva de la Ley de Servicios Digitales europea (LSDE, Reglamento 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un Mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)), que busca garantizar que lo que es ilegal en el mundo real lo sea también en el digital. Con el objetivo de cumplir con esta novedosa normativa, arranca oficialmente el Centro Europeo para la Transparencia Algorítmica (ECAT, por sus siglas en inglés) en Sevilla. La LSDE afecta a todos los operadores y plataformas de servicios digitales online, exigiéndoles informes de transparencia y auditorías (en las que deben explicar sus sistemas algorítmicos), requisitos sobre las condiciones de servicio, habida cuenta de los derechos fundamentales, cooperación con las autoridades nacionales de acuerdo con sus órdenes, Notificación y adopción de medidas y obligación de informar a los usuarios y mecanismos de reclamación, libertad de los usuarios para no recibir recomendaciones basadas en la elaboración de perfiles y prohibición de emisión de contenidos ilícitos, entre otras muchas. Porque están en riesgo derechos como la dignidad humana, la libertad de expresión y de información, incluidos la libertad de los medios de comunicación y su pluralismo, el derecho a la vida privada, el derecho a la protección de datos, el derecho a la no discriminación, los derechos del niño y la protección de los consumidores (Considerando 81 del Reglamento). El coordinador de servicios digitales de establecimiento o la Comisión pueden requerir acceso o informes relativos a datos específicos, incluidos los datos relacionados con algoritmos (Considerandos 96 y 141). Véanse también los arts. 14, 34, 35, 40, 69 y 72 del Reglamento. El ECAT deberá investigar también los efectos sociales a largo plazo de los algoritmos. La Comunidad de Madrid prevé abrir en 2024 su Instituto de Inteligencia Artificial, el primero autonómico a nivel nacional, para, entre otras cosas, estudiar la objetividad de los algoritmos.

esta normativa limitante por el resto de potencias mundiales), si no hay un diálogo real con USA y China, que serán los más reacios a aplicar estándares de seguridad similares, porque son ellas las potencias creadoras de sistemas de IA. Como dice Andrés Ortega, "los árbitros no ganan partidos"[20].

Los algoritmos se han usado siempre en la informática y sus sistemas operativos, en los programas informáticos y en las *apps* de los móviles. La última generación de ellos ha avanzado tanto que permite al sistema recopilar, preparar y analizar datos antes de gestionarlos y de dar recomendaciones o resultados. Es en ese proceso de preparación, de discriminación y de elección de datos en los que funcionan los sesgos, que el programador o diseñador del algoritmo puede haber introducido, para generar resultados no imparciales sino subjetivos. Esto es peligrosísimo y hace siempre necesaria la supervisión humana de los mismos, pues de lo contrario la legitimidad de la decisión queda comprometida[21].

Este riesgo de desviación (*bias*) algorítmica aumenta cuando hablamos del "deep learning", esto es, un subconjunto del aprendizaje automático, bien guiado por instrucciones humanas (*machine learning*, ML) o producido por el aprendizaje continuo de la misma máquina, mediante determinados sistemas de IA que implican el uso de redes neuronales artificiales con más de una capa oculta (*deep learning*, DL). En el aprendizaje automático, una red neuronal es una serie de sistemas computacionales interconectados, unidades organizadas en "capas", que aceptan múltiples entradas y producen una salida. Las redes neuronales profundas constan de varias capas. El aprendizaje automático de algunas IA ofrece modelos predictivos tras analizar la relación entre distintas variables mediante el análisis de un conjunto de datos, en aplicación de las leyes internas del algoritmo preestablecido y por medio de determinados criterios de clasificación. El algoritmo permite al aprendizaje automático aunar datos nuevos, que se suman a los antiguos, en un volumen cada vez mayor, de forma que parece que "aprende" por sí mismo, aunque en realidad no está sacando conclusiones propias sino las que predetermina el sistema. Por eso "aprendizaje automático" es otro oxímoron. Sí cabe hablar de mejora o afinamiento de los resultados, porque la información nueva mejora la antigua y la completa. Y el sistema tiene en cuenta sus propias conclusiones, que se añaden a los nuevos datos, y así progresivamente. En teoría, la ML tiende a la omnisciencia, pero nunca podrá usar esos datos de forma humana. De ahí también su riesgo.

Compartimos con Eguíluz Castañeira la necesidad de chequear la objetividad de los algoritmos, algo que podría hacerse derivar de la evaluación de Impacto de Protección de Datos del art. 35 del Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), siguiendo también las indicaciones de la FRA (Agencia de la UE para los Derechos

20. Cfr. Ortega 2021, p. 5.

21. En dos Informes de la European Union Agency for Fundamental Rights (FRA), titulados *BigData: Discrimination in data-supported decision making* (2019) y *Bias in algorithms. Artificial inteligence and discrimination* (2022), la UE reconoce que las herramientas automatizadas están lejos de ser neutrales, y no son necesariamente menos discriminatorias, de forma que "el sesgo forma parte del desarrollo de algoritmos". Por tanto, es muy posible y ocurre a menudo que el uso de algoritmos para tomar decisiones pueda vulnerar derechos humanos. El sesgo es algo tan sutil que el algoritmo puede estar preparado para que el mismo no aparezca al principio, sino que se vaya desarrollando con el paso del tiempo. Esos dos informes caminan más bien por la denuncia del sesgo algorítmico cuando produce resultados políticamente incorrectos. También puede producirse un sesgo debido a que los datos con los que se alimenta al algoritmo sean defectuosos o parciales. Sin embargo, es más peligroso incluso, consideramos nosotros, cuando el sesgo está creado para ocultar deliberadamente resultados políticamente incorrectos. Los sesgos pueden producirse hacia un lado o hacia el otro. Lo importante es que los algoritmos no tengan sesgos, y que arrojen resultados objetivos e imparciales conforme a los datos objetivos que se les introducen, aunque sean políticamente incorrectos. Una forma de dar resultados desviados es obviar determinados datos, como indica Harari 2017, p. 430.

fundamentales)[22], que permitiría crear auditorías periódicas de algoritmos, que analicen "desde un punto de vista ético-jurídico el recorrido de todas sus fases: diseño, tratamiento, resultado; a través de agencias de certificación o expertos independientes" e imparciales.

Por ejemplo, a nivel español, se encargaría la Agencia Española de Supervisión de la Inteligencia Artificial, que tiene su sede física en La Coruña, y estará en funcionamiento en pocos meses; y a nivel europeo, el Centro Europeo de Transparencia algorítmica, con sede en Sevilla, con la intención de eliminar sesgos y prevenir posibles efectos discriminatorios. Nos unimos también a Eguíluz en su recomendación de establecer además una atribución de responsabilidades a los informáticos y programadores (y a las empresas que le dieron las instrucciones para elaborarlos). Las empresas que utilizan algoritmos deben dar información suficiente, concisa y de fácil comprensión a los interesados, tanto a sus usuarios como a las personas cuyos datos personales son tratados, haciendo efectivo el derecho al acceso a la información y a su vez los derechos del artículo 22 RGPD[23]. A nivel de Administraciones públicas y del sector público, esta información debería ser información institucional, colgada de sus páginas web.

A los efectos procesales, la IA puede enlazar y encontrar patrones entre la veracidad o falsedad de las declaraciones de un testigo con datos relacionados con su edad, raza, sexo, religión, etc., incluso con datos biométricos[24] o de salud, mediante datos inferidos. Y, como indica PÉREZ ESTRADA, el sujeto podría dar esos datos sin saber que serán usados por la IA para inferir su conducta procesal con los mismos[25]. Consideramos que este "perfilado" o *profiling* de los sujetos procesales es ilegal e inconstitucional porque puede dar lugar a la ruptura del principio de presunción de inocencia y al de igualdad. Así lo ha establecido el art. 22 del Reglamento (UE) 2016/679, del Parlamento europeo y del Consejo, de 27 de abril de 2016 (RGPD), en el que se prohíbe que un administrado esté obligado a aceptar una decisión basada únicamente en el tratamiento automatizado de datos (por ejemplo, en un ODR, *online dispute resolution* o juicio electrónico), incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, sin su consentimiento. Es decir, el administrado puede negarse (también puede aceptarlo), ya que le asiste el derecho a obtener la intervención humana por parte del responsable (el juez o el funcionario de turno), a expresar su punto de vista y a impugnar la decisión obtenida mediante IA. Más recientemente, el Considerando 44 de la propuesta de Reglamento IA de la UE contempla que los sesgos pueden ser inherentes a los conjuntos de datos subyacentes[26].

Cathy O'Neil aboga por la necesidad de entrenar los algoritmos permanentemente, de forma

22. Cfr. FRA, *Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales*, resumen, p. 7. La FRA ha confirmado las prácticas ausencia de evaluaciones en profundidad sobre la discriminación de colectivos vulnerables, en el diseño de la IA (p. 10).

23. Cfr. Eguíluz Castañeira 2020, p. 360.

24. La Resolución del Parlamento Europeo de 3 de mayo de 2022, titulada *Inteligencia artificial en la era digital*, advierte de que es propio de dictaduras el control biométrico de la población, y que su uso en áreas militares o en el poder judicial es contradictorio con los valores europeos: «Destaca que muchos regímenes autoritarios utilizan sistemas de IA para controlar, espiar, seguir y clasificar a sus ciudadanos, restringir su libertad de circulación y ejercer vigilancia colectiva; hace hincapié en que cualquier forma de marcaje normativo ciudadano por parte de las autoridades públicas, especialmente en el ámbito de las fuerzas de seguridad del Estado, el control de las fronteras y el poder judicial, así como su uso por parte de empresas privadas o particulares, conduce a la pérdida de autonomía y privacidad y no está en consonancia con los valores europeos».

25. Cfr. Pérez Estrada 2022, p. 35.

26. Especialmente cuando se utilizan datos históricos, introducidos por los desarrolladores de los algoritmos o generados cuando los sistemas se aplican en entornos del mundo real. Los resultados de los sistemas de IA dependen de los sesgos inherentes que tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados grupos vulnerables o étnicos o comunidades racializadas.

que los ingenieros informáticos y los matemáticos los chequeen para ver si producen aberraciones. Da noticia de que se están creando soluciones para auditar de forma anónima los algoritmos, como está haciendo la Universidad de Princeton, que ha creado un software que se hace pasar por una persona anónima y que se hace usuaria del algoritmo, para ver si es justamente tratada. También lo están haciendo Universidades como Carnegie Mellon y el MIT[27].

3. Las bases de datos y sus riesgos

Comienza a ser habitual en los cuerpos y fuerzas de seguridad, y, por ende, en juzgados y tribunales, sobre todo en los penales, aunque también en procesos contencioso-administrativos con objeto sancionador el uso de bases de datos *(big data*), que no se refieren aquí a las bases de datos de legislación, jurisprudencia o doctrina sino a bases de datos fácticos, relativos a hechos, circunstancias, opiniones vertidas en redes sociales u obtenidas de las aplicaciones de los smartphones, fotos y filmaciones de cámaras policiales o de otras cámaras públicas, delitos o infracciones administrativas (y su ubicación, instrumentos con los que se comete, personas implicadas y culpables, fechas de comisión) que determinadas máquinas de IA manejan y manosean hasta inducir patrones, estadísticas, perfiles de personas y predictibilidad de delitos e infracciones.

Es lo que en USA se llama *predictive policing* (o *PredPol*), que se ha extendido por estados como California, Washington, Carolina del Sur, Alabama, Arizona, Tennessee, NY o Illinois, en UK en el Condado de Kent, y en los Países Bajos[28]. Y en China a todas horas y lugares, no sólo para evitar la criminalidad sino como herramienta comunista de control social, incluso con ocasión del covid[29]. No es casual que el único Estado que ha desarrollado jueces robot, sustituyendo a los jueces persona en todo el proceso sea China[30].

Por cierto, lo que ocurrió en tiempos del Covid, con Estados paranoicos que segregaban a los que no se vacunaban de unas terapias genéticas no probadas adecuadamente es un buen ejemplo de que este estado de vigilancia total[31] no es ciencia ficción, que adopta decisiones de carácter político escondidas bajo la veste de supuestas amenazas sanitarias, que tiene ya la capacidad técnica absoluta como para poder implementarlo. El *Leviathan*

27. Cfr. O'Neil 2017, p. 260.
28. Otros similares son *Compstat* en Nueva York o HunchLab en Filadelfia. En el capítulo 5° de su libro, titulado *La justicia en la era del big data*, Cathy O'Neil advierte de cómo este tipo de programas predictivos es eficaz, porque la policía recibe una cuadrícula por dónde patrullar preferentemente para evitar delitos de alteración del orden público, lo que es ciertamente un avance, pero que se muestra ineficaz para perseguir otros delitos, como los económicos. Cfr. O'Neil 2017, pp. 108-114.
29. Cfr. Barona Vilar 2021, pp. 450-451.
30. Los llamados Tribunales o Cortes de Internet, en Hangzhou, desde 2017, para disputas acaecidas en Internet, como contratos, préstamos, disputas de dominios de Internet, difamación por Internet. Luego se han abierto también en Pekín y en Guangzhou. Se tramitan miles de casos al año, con una duración de 38 días, pero, ¿a qué coste de los derechos fundamentales y de las garantías procesales?
31. El poder público animaba a los ciudadanos a instalar en sus propios teléfonos móviles aplicaciones que les ubicaban, que indicaban el tiempo que pasaban en determinados lugares, que supuestamente informaban de la cercanía de personas no vacunadas, que limitaban los movimientos de los no vacunados, que indicaban si se había cumplido el tiempo de desconfinamiento, con drones que detectaban la temperatura corporal de la gente (o con arcos a la entrada de recintos)… y todo eso lo hemos visto, y muchos lo han aceptado, sin ser conscientes de que se trataba de un inmenso experimento de control social y de testeo de la docilidad ciudadana a su imposición. Como experimento, se ha demostrado sobradamente que el poder público, con la excusa del miedo, puede imponer sin apenas contestación pública, un estado de vigilancia digital completo, arrasando derechos fundamentales como la intimidad, el derecho a la libertad de circulación, libertad de manifestación o de reunión, e incluso de expresión. Recordemos que en España se activó el rastreo de nuestros móviles como medida de urgencia, activada por la Secretaría de Estado de Digitalización e Inteligencia artificial y el Ministerio de Asuntos económicos y Transformación digital (BOE, 28 de marzo de 2020).

algorítmico está aquí ya, como un enorme elefante en la habitación[32].

El riesgo aquí es que el juez les otorgue a las conclusiones así obtenidas mediante IA una especie de presunción de veracidad *iuris et de iure*, sin discutir sus resultados o sin comprobarlos. Nunca debería ser así porque es muy posible que la calidad de los datos recopilados sobre los que la máquina aplica su algoritmo pueda no ser cierta del todo o ser incorrecta, lo que daría lugar a resultados con sesgos imperceptibles al cerebro humano, pero ciertamente existentes[33].

El uso de estas bases de datos otorga un poder sin precedentes a las empresas, Administraciones, Universidades, empleadores, ONGs, policía, partidos políticos, etc. que las utilicen, pues permiten tener una visión sin precedentes del comportamiento humano, de la vida privada y de nuestras sociedades. La tentación es grande pues una rápida consulta a estas bases de datos nos permitiría tener un perfil rápido de un candidato a trabajar en una empresa, de un profesor a contratar en una Universidad, de los alumnos que solicitan ingresar en ella, de sospechosos de comisión de delitos o de infracciones administrativas, e incluso, en el ámbito procesal, de la veracidad de un testigo, de la predictibilidad de las resoluciones de un juez, de la legalidad de los actos administrativos de un determinado funcionario o ayuntamiento, etc.[34] Como se puede imaginar, los ámbitos de empleo de esos datos son muy sensibles y su uso puede afectar claramente a los derechos fundamentales a la igualdad, a la privacidad o a la libertad de expresión, religión, filiación política, etc. Y si hablamos del proceso, de la igualdad de las partes, de la presunción de inocencia, de la imparcialidad y objetividad del juez e incluso al juez predeterminado por ley. Porque las máquinas no son imparciales, sino subjetivas, tal y como lo son los algoritmos que las impulsan, diseñados por hombres.

De ahí la necesidad de que el juez use estas bases de datos como muleta o ayuda, y compruebe con "criterio humano" las soluciones propuestas por la inteligencia artificial. Corremos, caso contrario, el riesgo de pasar del *Iura novit curia* al *Iura novit machina*.

4. La informática jurídica decisional y la predictiva o de perfilado

Siguiendo a Suárez Xavier, las herramientas de IA aplicadas al sistema judicial se pueden clasificar en algoritmos propios del sistema judicial (empleados por los jueces, y, a veces, también diseñados y desarrollados por el sistema judicial) y algoritmos o sistemas periféricos, usados por prestadores privados de IA y que emplean los profesionales que trabajan en el entorno judicial, como abogados, procuradores, trabajadores sociales y peritos[35].

Las herramientas de IA propias del sistema judicial podemos clasificarlas entre las que dan soporte al juez y las de tramitación administrativa o procesal, clasificación que sigue el espíritu de la Ley 13/2009, de Reforma de la Legislación procesal para la implantación de la nueva Oficina judicial. Y dentro de las que dan soporte al juez las hay de carácter

32. De la misma opinión son Simoncini-Longo 2021, p. 29.

33. En la Resolución del Parlamento Europeo titulada *Implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)), de 14 de marzo de 2017, se definen los macrodatos como la «recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos)» y denuncia que «los datos de capacitación a menudo son de una calidad cuestionable y no son neutrales».

34. En esta Resolución del Parlamento Europeo de 14 de marzo de 2017 se explica que esos conjuntos de datos y la analítica de macrodatos se emplean para estimular la competitividad, la innovación, la prospección del mercado, las campañas políticas, la publicidad selectiva, la investigación científica y la elaboración de políticas en los ámbitos del transporte, la fiscalidad, los servicios financieros, las "ciudades inteligentes", la aplicación de la ley, la transparencia, la salud pública y la respuesta a las catástrofes, así como para influenciar las elecciones y los resultados políticos, por ejemplo mediante comunicaciones específicas…

35. Cfr. Suárez Xavier 2023, p. 107.

de apoyo al Juez (sistemas de IA asistenciales, o de *Decision Support*[36]), que tienen que ver con el manejo avanzado de bases de datos de jurisprudencia, doctrina legal y doctrina académica, y las avanzadas, de experto o *deep learning*, que pueden dar soluciones acabadas al juez o establecer elementos de juicio para la toma de decisiones, como el perfilado y la justicia predictiva (aquélla en la que se hacen perfiles y estadísticas sobre los jueces y magistrados, relacionados con sus decisiones en distintos asuntos según la materia).

Las soluciones jurídicas ofrecidas por la IA acarrean un grave problema de motivación, porque el juez no siempre está en condiciones de poder explicar por qué se ha tomado una decisión concreta, que le viene dada por la IA. En realidad, el *deep learning* no es exactamente un sinónimo de "sistema experto de IA" pues ése es un sistema algorítmico que imita el funcionamiento del cerebro humano mediante redes neuronales artificiales, que se componen a su vez de cientos de capas de neuronas, cada una de las cuales recibe e interpreta información de la capa anterior. Y éste (el sistema experto) es un tipo de *deep learning* en el que el usuario se relaciona con la máquina por medio de una *interface* que se materializa haciéndole preguntas al sistema, que acaban funcionando a modo de silogismo, emulando también el razonamiento, si se puede decir así, de un funcionario que aplica una norma o de un juez[37].

El uso de la IA como herramienta de apoyo al Juez, mediante un uso proporcional, herramientas auxiliares derivadas de bases de datos y de herramientas de recopilación y búsqueda de legislación, jurisprudencia y doctrina, no acarrea mayor problema. En esto los jueces no se diferencian a otros operadores jurídicos. La diferencia la marca el paso de estas herramientas de ayuda a herramientas decisionales, es decir, a sistemas de IA que con *deep learning*, aprendizaje automatizado y otras funcionalidades permiten a la máquina elaborar resoluciones, sentencias, autos, providencias, desestimaciones, etc., por su capacidad para redactar a partir de la lectura de los documentos presentados por las partes. Como decíamos arriba, la tentación de los jueces de emplear estas herramientas es muy grande, pues el atasco de las jurisdicciones en España es brutal, sobre todo en el contencioso-administrativo, y la eficacia y eficiencia que su uso produciría le permitiría a jueces y magistrados llevar una vida laboral menos estresante.

La Justicia está transitando (no aún en España pero sí en otros países) de la *informática jurídica documental* de las bases de datos y de las recopilaciones jurídicas a la *informática jurídica de gestión* o *administrativa* (que permite un mejor reparto de trabajo o el empleo de modelos de escritos, a la presentación y comunicación de escritos por vía telemática y a la interrelación de las partes por vía telemática, incluyendo la posibilidad de videoconferencias) a esta *informática jurídica decisional*.

En España se están tomando algunas iniciativas en los sistemas de informática jurídica documental y de gestión aplicada al proceso, basada en la interoperatividad y digitalización de la justicia (informática jurídica de gestión o administrativa), pero aún no llega a ser IA experta o decisoria:

– El Convenio marco de colaboración entre el CGPJ y el Ministerio de Energía, Turismo y Agenda Digital, de 13 de octubre de 2017, para el impulso e incorporación de tecnologías del lenguaje en el ámbito de la justicia, que usa la base de datos del CENDOJ para un mejor tratamiento de legislación y jurisprudencia y traducción automática de textos en otros idiomas.
– El proyecto de Proyecto de Ley de Medidas de eficiencia procesal del servicio público de Justicia, ya caducado, que trataba de regular la transformación digital de la Justicia, estableciendo un marco jurídico de vanguardia para promover y facilitar el avance en la transformación digital, regulando los servicios digitales accesibles a la ciudadanía, reforzando la seguridad jurídica en el ámbito digital, impulsando su eficiencia y orientando al dato los sistemas de Justicia. La ley pretendía fortalecer

36. Los *Decission Support Systems* (DSS) se usan en USA para casos sencillos, en los que la IA ofrece distintas alternativas de resolución, entre las que escoge el juez. Indica además los preceptos legales y la jurisprudencia aplicables. Cfr. Murillo Paños 2021, pp. 319-320.

37. Como indican Vélez-Quinteros 2023, p. 216, los sistemas de IA deben ser entrenados por humanos, que purguen sus errores o aberraciones. El art. 15.4 de la propuesta de Reglamento IA de la UE aboga por ello.

la interoperabilidad de los sistemas existentes mediante el intercambio y la transmisión de documentos electrónicos entre órganos judiciales o fiscales. En este sentido, contemplaba la potenciación del expediente judicial electrónico o digital[38], por el que se pasaba de la orientación al documento a la orientación al dato, es decir, a la transcripción de los documentos[39] y el dictado jurídico[40].

La informática jurídica decisional o *artificial legal intelligence* (ALI) se realiza mediante los denominados "sistemas jurídicos expertos", aunque sus escritos y resoluciones nunca deben tener la última palabra sino ser siempre chequeados y servir de fundamento (o no) para las verdaderas resoluciones judiciales, que siempre deben ser humanas[41].

Estos sistemas le facilitan al abogado o al juez que los utilice mejorar la argumentación jurídica, pues se adentra en la creación jurídica, redacción de escritos, motivación de los mismos, etc. Ya no estamos sólo en una organización o criba de información sino en la obtención de datos para hacer propuestas[42].

De nuevo, cabe decir que los operadores jurídicos (entre ellos los jueces) desconocemos el modo en que estos sistemas de IA llegan a las conclusiones o soluciones que nos ofrecen, y eso las hace opacas y generan *inseguridad jurídica* pues no cabe una completa motivación del resultado por parte del juez, sino sólo la explicación inmediata de la jurisprudencia, doctrina o legislación empleada. Esa opacidad puede arrojar sobre los jueces ciertas dudas de parcialidad, ya que los sesgos u omisiones derivadas del empleo de la IA pueden afectar a las sentencias y acabar con el derecho fundamental a la imparcialidad judicial, por ejemplo.

En España no se usan aún estos sistemas jurídicos expertos, como sí ocurre en USA con COMPAS (*Correctional Management Profiling for Alternative Sanctions*), que es un sistema de perfilado o predictivo[43], o WATSON (desarrollado por IBM) o *Tax Foresight*, desarrollado por la

38. EL art. 230 LOPJ establece la obligatoriedad del empleo por juzgados, tribunales y fiscalías de cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establece la propia LOPJ en materia de protección de datos de carácter personal y en la normativa orgánica de protección de datos personales. Este precepto ha sido desarrollado por el Acuerdo de 22 de noviembre de 2018, de la Comisión Permanente del Consejo General del Poder Judicial, por el que se aprueba la Instrucción 1/2018, relativa a la obligatoriedad para Jueces y Magistrados del empleo de medios informáticos a que se refiere el artículo 230 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Esta Instrucción establece los requisitos técnicos mínimos para que los programas informáticos de gestión procesal puedan usarse. Entre ellos, claro está, cabría incluir a los sistemas de IA de gestión. La aprobación definitiva de los correspondientes programas corresponderá a las Administraciones competentes, pero su utilización no podrá imponerse como obligatoria a jueces/zas y magistrados/as si no se satisfacen los requisitos técnicos que permiten imponer esa obligación.
39. Esa orientación al dato permitirá actuaciones automatizadas, proactivas y asistidas, aunque siempre con el respeto pleno a las leyes procesales y bajo criterios legales objetivos y públicos, atendiendo a la importancia que tiene para la sociedad obtener resoluciones judiciales en un plazo razonable. De igual forma, la preferencia por las comunicaciones judiciales telemáticas, siempre en condiciones de plena seguridad jurídica, tendrá similar orientación al dato, previéndose mecanismos para la transmisión de comunicaciones masivas.
40. Esta solución ya existe en España, diseñada por el Ministerio de Justicia, y emplea capas neuronales profundas y le permite a jueces y magistrados, letrados y fiscales la posibilidad de realizar de forma rápida y precisa transcripciones especializadas de textos jurídicos, utilizando el software de reconocimiento de voz y traducción, posibilitando el uso de términos jurídicos. Cfr. Olmedo Palacios 2023, p. 713.
41. Algunos de los primeros fueron el *Watson*, de IBM, el *Ross*, o el *Debater*. Actualmente hay otros capaces de analizar textos y extraer conclusiones de ellos, como *Ravel Law*. Otros pueden redactar escritos e informes, como *Lawdepot*. Otros pueden transcribir las intervenciones orales de testigos, peritos, abogados y jueces, como *Digalaw*. Y otros muchos, de predicción, valoración, negociación o resolución online de disputas (eConciliación, Mediaré, Redalyc), etc.
42. Cfr. Barona Vilar 2021, p. 361.
43. Con algunos datos no directamente relacionados con el delito, como el teléfono de la casa, dificultad para pagar facturas previas, antecedentes familiares, etc.

Empresa Blue J. Legal, o el SSPS (IBM), que se usa en el sistema de delincuencia juvenil de Florida, para reducir la reincidencia de menores. También existen sistemas como RAVEL LAW o ROSS *chatbot* También existe HART (*Harm Assessment Risk Tool*), desarrollada en la Universidad de Cambridge, para evaluar el riesgo de reincidencia de sospechosos, en base a una treintena de factores (minería de datos, *data mining*), algunos de los cuales no están relacionados con el delito (v. gr., código postal de residencia o sexo[44]).

En Australia se usa el sistema experto *Split-up*, para ayudar a los jueces a la partición de bienes tras un divorcio; en Méjico el *Expertius*, para liquidar el patrimonio conyugal; o *Sies*, que ayuda al juez en juicios de divorcio, patria potestad y alimentos[45]. Y en España, *VeriPol*, un sistema implantado en 2018 por la Policía Nacional para detectar denuncias falsas[46].

Evidentemente, de la cantidad masiva de datos que puede usar una herramienta de IA predictiva o de perfilado no todos han sido cedidos voluntariamente por los interesados. Muchos proceden del propio sistema administrativo y/o judicial[47] (pero no pueden ser exhibidos públicamente porque son datos privados, necesarios para el proceso; en teoría tampoco deberían ser tratados en el proceso sin autorización del afectado), otros se obtienen de las redes sociales (en las que tan alegremente la gente deja sus datos y opiniones más íntimas), otras veces se obtienen con engaños más o menos velados, en no menos veces se compran y se venden por parte de las empresas (práctica habitual en USA) y en ocasiones directamente se roban[48]. Estamos en el mundo del bazar de los datos, un gran mercado persa donde todo se compra y se vende, mercado en ebullición desde la aparición de la IA, que necesita los datos como combustible para poder funcionar.

También en Estonia y China se usan, para pleitos de cuantía inferior a 7.000 euros y como robot de asistencia a letrados, partes y jueces, respectivamente[49]. Y en Argentina, el sistema PROMETEA, que, al menos, no usa "cajas negras" (*black boxes*) para sus labores predictivas, de asesoría, simplificación y organización, pues el algoritmo es visible y obtiene resultados por analogía o por lógica de premisa-consecuencia[50]. Y es que, a mi juicio, lo fundamental de estos sistemas de IA predictivos y decisorios es que no pueden ser opacos, y lo son en la mayoría de los casos por razones de patentes y propiedad intelectual[51]. En la UE debería

44. HART arrojó un 98% de fiabilidad para la predicción del riesgo bajo de reincidencia y de sólo el 88% en la del riesgo alto. Cfr. Consejo de Europa 2018.

45. Cr. Ayllón García 2020, p. 9.

46. Con un 80% de aciertos. Cfr. Tierno Barrios 2020.

47. Datos del expediente administrativo requerido por el Juez; datos generados en el mismo proceso durante el litigio, aportados por las partes y por el Juez, tanto en sus escritos como en la prueba; datos aportados desde fuera, mediante periciales, prueba documental o testifical. Estos datos son muy golosos para los sistemas de IA, en su inmensa mayoría privados y comerciales, y la Justicia traicionaría su propia misión si los cediera a terceros. De todos estos datos, sólo los mínimos datos personales necesarios para comprender la sentencia y su *ratio decidendi* deben trascender en las sentencias y demás resoluciones judiciales, pues CENDOJ y otras bases de datos como ARANZADI, Westlaw, Vlex, Tirant, Wolters-Kluwer, etc. los recopilan legalmente y es desde ellas que esos datos pueden trascender al público y al mercado. Por eso el nuevo Considerando 45 *bis*, introducido por el Parlamento europeo en la propuesta de Reglamento IA de la UE indica que los proveedores y los usuarios de sistemas de IA deben aplicar medidas técnicas y organizativas conforme al estado de la técnica al objeto de proteger esos derechos (privacidad y protección de datos personales). Dichas medidas deben incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología cada vez más disponible que permite introducir algoritmos en los datos y obtener información valiosa sin la transmisión entre las partes ni la copia innecesaria de los propios datos en bruto o estructurados.

48. Cfr. Moreno Catena 2022, p. 49.

49. Cfr. Pérez Estrada 2022, pp. 65-66.

50. Puede profundizarse en su explicación leyendo Hernández-Font-Santiago 2020.

51. En el caso Loomis v. Wisconsin (2016), el Sr. Loomis fue detenido tras robar un coche y huir de la policía. El fiscal presentó un informe elaborado con un sistema de IA de perfilado llamado COMPAS, desarrollado por la empresa privada Northpointe Inc., sobre su peligro de reincidencia, que sirvió al Tribunal para condenarle a una pena

someterse la patente a la debida transparencia, al menos en procesos judiciales. Y obligar a los diseñadores y empresas de IA no sólo a enseñar los algoritmos (código fuente) sino explicar cómo se llega a los resultados o información de salida (trazabilidad o cognoscibilidad).

En Brasil se emplea también un sistema de *machine learning* para la toma de decisiones judiciales, mediante dos sistemas de IA llamados "Víctor" y "Sócrates", que actúan en el Supremo Tribunal Federal (nuestro TC) y en el Superior Tribunal de Justicia (nuestro TS), desde 2018. Son sistemas avanzados, de redes neuronales. En el primero, el sistema consigue identificar casos que puedan ser de interés general, requisito necesario para la admisión de los recursos extraordinarios. Cabría aquí también aplicar sistemas de IA que sirvan de filtro para ayudar a los magistrados a detectar el interés casacional en España (por la afectación al interés general de una determinada materia con elementos de juicio nuevos y/o por ser casos nunca resueltos hasta el momento con alto impacto social) de un asunto. En el segundo, el sistema identifica los recursos similares y los agrupa. Ninguno de los dos sistemas toma decisiones por sí mismos: las apuntan, pero requieren de un juez que las acepte, por lo que no se conculca el derecho a un juicio justo, que sólo lo puede garantizar un ser humano.

A nivel europeo, el proyecto de Reglamento de IA de la UE consideraba la elaboración de perfiles y de probabilidad de reincidencia mediante IA como sistemas de alto riesgo. Luego los ha prohibido, por enmiendas del Parlamento, dentro del proceso o en vía administrativa, en el art. 5. 1, d) *bis* de la propuesta. Y en el Considerando 26 *bis*[52].

Estos sistemas de IA predictivas o de perfilado, evidentemente, sólo se usan por ahora en la jurisdicción penal de otros países pero, hasta la prohibición europea antes señalada, era razonable pensar que pudieran acabar siendo utilizados también en la jurisdicción contencioso-administrativa a la hora de valorar el riesgo de reincidencia, a la hora de otorgar medidas cautelares contra el acusado, en materia de infracciones y sanciones. Aquí se hubieran comprometido gravemente derechos fundamentales del proceso como la igualdad, la intimidad o privacidad, a un juicio justo, tutela judicial efectiva, juez imparcial, presunción de inocencia, proporcionalidad, etc. De ahí la importancia de que el Juez revise las soluciones ofertadas por la IA y que conozca el proceso intelectivo realizado por el algoritmo, al menos en sus elementos fundamentales. Es por eso por lo que Martín Diz considera que la regulación que se haga de la IA aplicada al sistema judicial debe impedir que los llamados "derechos procesales fundamentales", esto es, las garantías procesales, sean vulnerados

de 6 años de prisión y otros 5 en régimen de libertad vigilada, ya que el informe concluía que el condenado representaba un "alto riesgo para la comunidad". La defensa del condenado recurrió alegando que se había vulnerado el derecho a un proceso con todas las garantías (*due process*) porque no podía discutir los métodos utilizados por el programa informático Compas dado que el algoritmo era secreto y solo lo conocía la empresa que lo había desarrollado. Sin embargo, tales argumentos no fueron acogidos por la Corte Suprema del Estado de Wisconsin, y tampoco el Tribunal Supremo admitió el recurso. En el caso State of Arkansas v. John Ketih Walls (2017) el tribunal sí concedió al Sr. Walls el derecho a acceder al informe de riesgo, como es propio de todo Informe pericial previo a la sentencia, pero no se concedió tampoco el acceso al algoritmo, por las mismas razones que en el caso Loomis. Habría que decir que tomar estas decisiones sobre la libertad provisional de un preso conforme a un análisis matemático de porcentajes es algo realmente peligroso, pues en esas operaciones entran en juego no sólo factores personales del reo (delitos previamente cometidos, antecedentes de fuga, etc.) sino también sociales (religión, clase social, lugar de residencia, ingresos) e incluso biométricos (raza, sexo). Y los algoritmos suelen fijarse en todos estos detalles para obtener ese porcentaje.

52. Anexo III, apdo. 6, e), que decía así «sistemas de IA destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para predecir la frecuencia o reiteración de una infracción penal real o potencial con base en la elaboración de perfiles de personas físicas, de conformidad con lo dispuesto en el artículo 3, apartado 4, de la Directiva (UE) 2016/680, o en la evaluación de rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos». Sin embargo, el Parlamento europeo ha suprimido ese apartado y ha prohibido esos sistemas de IA.

por la implantación irrefrenable y poco planificada de los sistemas de IA[53]. Ese riesgo, como indica el Considerando 38 de la propuesta de Reglamento IA de la UE motiva su inclusión de los sistemas de IA en el ámbito judicial como de alto riesgo.

El RGPD permite la elaboración de perfiles (perfilado), siempre que el afectado hubiera consentido a entregar los datos, que es «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». Pero no permite decisiones que le afecten que se basen sólo en el tratamiento automatizado de dichos datos si no hay una supervisión de una persona al respecto[54,55].

Y esos datos personales nunca pueden ser datos del origen étnico o racial, de las opiniones políticas, de las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física (art. 9.1 del Reglamento). Esto se hace para evitar sesgos, pero puede ocurrir que el algoritmo los emplee, si le fueron suministrados de manera accesoria, sin que la Administración o el Juez-Magistrado lo sepa, por la opacidad de las "cajas negras" del mismo. Podríamos llegar al horror de una especie de *criptonomia*. En estos casos, evidentemente, se producen discriminaciones que no pueden ser asumidas en el proceso y este tipo de algoritmos opacos deberían ser prohibidos, salvo que se pueda tener acceso a los mismos por parte de las partes en el pleito[56]. De ahí que los sistemas de *deep learning* con cajas negras están prohibidos en la UE porque impiden la motivación y la transparencia de las resoluciones administrativas y judiciales. Cada vez más empresas están programando algoritmos con "cajas blancas" que, aunque menos potentes, explican mediante árboles de decisión todos los pasos seguidos por la máquina para llegar a la solución propuesta[57]. Desde luego, en el sistema judicial, éstos últimos deberían ser los únicos permitidos.

53. Cfr. Martín Diz 2019, pp. 815-827.

54. No obstante esa prohibición, recogida en su art. 22.1, los apartados siguientes de dicho artículo permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor. Entre las medidas que se le piden al responsable del tratamiento está la adopción de las «medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable».

55. También lo prohíbe el art. 11 de la Directiva 2016/680, del Parlamento europeo y del Consejo, de 27 de abril, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

56. En general, si las partes en un proceso no pueden acceder al algoritmo o a una explicación sencilla de cómo funciona se estaría vulnerando el derecho a la interdicción de la arbitrariedad del art. 9.3 CE. Cfr. Berning-Prieto 2023, pp. 114-115.

57. Cfr. Salazar García 2022, p. 61.

5. Límites éticos y jurídicos al empleo de la IA en el proceso judicial

En la actualidad no hay normativa ni estatal ni autonómica sobre el uso de la IA en el proceso judicial. A nivel europeo sólo existen unas breves prescripciones en el proyecto de Reglamento IA de la UE. Y *soft law* de carácter internacional, que ahora veremos. Haremos, pues, algunas reflexiones *de lege ferenda*.

La existencia de una Agencia independiente estatal que compruebe la corrección y legalidad de los algoritmos ha sido aconsejada por Ives Gaudemet[58], por expertos de control de sistemas y juristas. Quizás esa labor pueda desempeñarla el Comité técnico estatal de la Administración judicial electrónica, dentro del marco que pueda establecer la DG de Transformación digital de la administración de Justicia (art. 6 del RD 453/2020[59]).

Es muy importante citar una fuente de *soft law* muy relevante como es la Carta Ética Europea sobre el uso de inteligencia artificial en los sistemas judiciales, adoptada por el Consejo de Europa, en concreto por la Comisión Europea para la eficiencia de la Justicia (CEPEJ) los días 3 y 4 de diciembre de 2018, cuyos principios han quedado resumidos en el punto XXV de la Carta de Derecho digitales del Ministerio de Asuntos Económicos y Transformación digital de 2021[60]; y el Libro Blanco Europeo sobre inteligencia artificial (con el ampuloso título de "Un enfoque europeo orientado a la excelencia y la confianza"), Bruselas, 19 de febrero de 2020, COM(2020) 65 final.

Especialmente importante es la *Carta Ética del Consejo de Europa*, que intenta crear una *ciberética* mediante el establecimiento de cinco principios esenciales para el uso de herramientas de IA en el ámbito judicial:

- El principio de respeto de los derechos fundamentales, cuya finalidad es asegurar que el diseño y la implementación de las herramientas y servicios de inteligencia artificial son compatibles con los derechos fundamentales. Se han de respetar los derechos del Convenio Europeo de Derechos humanos y del Convenio n. 108 del Consejo de Europa, sobre Protección de datos personales.
- El principio de no discriminación, que informa a favor de la prevención de cualquier discriminación entre individuos o grupos de individuos, fundamentalmente mediante el uso de datos personales que pudieran provocar sesgos en los resultados propuestos (sobre todo, en sistemas de perfilado o *profiling*).
- El principio de calidad y seguridad, que aboga que, en el procesamiento de decisiones judiciales y datos, se usen fuentes certificadas y veraces y datos intangibles con modelos concebidos en un sistema multidisciplinario (es decir, que en el diseño del algoritmo participen órganos compuestos por jueces, investigadores en ciencias sociales e informáticas, tanto en la fase de redacción, como de dirección y aplicación), en un entorno tecnológico seguro. Los algoritmos deben ser registrables y rastreables en todo momento y ejecutarse en entornos seguros, no hackeables.
- El principio de transparencia, imparcialidad y equidad, de forma que los métodos de procesamiento de datos (algoritmos) sean transparentes, accesibles y comprensibles, para el que lo emplea y para los administrados afectados,

58. Cfr. Gaudemet 2018, pp. 651-664.

59. Este RD desarrolla la estructura orgánica básica del Ministerio de Justicia, y se modifica el Reglamento del Servicio Jurídico del Estado, aprobado por el Real Decreto 997/2003, de 25 de julio.

60. El punto XXV recoge, como *soft law*, los derechos de los usuarios españoles ante la inteligencia artificial. El primero es el respeto de esos sistemas a la dignidad humana, al bien común y al principio de no maleficencia. Lamentablemente, el empleo de la IA puede provocar daños graves a nivel jurídico si no se controla adecuadamente. Consagra también esta Carta el derecho a la no discriminación, evitando los sesgos que estos sistemas pueden tener; también se les exige cumplir con condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible. También, los sistemas de IA deberán garantizar la accesibilidad, usabilidad y fiabilidad de los algoritmos. Finalmente, las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.

susceptible de auditorías externas (que otorgarían la certificación periódica de la transparencia y neutralidad de los algoritmos). La protección de la propiedad intelectual debe ser compatible con el acceso a los algoritmos ya que se debe priorizar el interés público de una justicia objetiva y de calidad. Todo esto debe ser explicado en lenguaje entendible para jueces y usuarios.

– Y el principio "bajo control del usuario", que se asegure que los usuarios estén informados, por ejemplo, de que el juez o la Administración están empleando sistemas de IA[61], y del carácter vinculante o no del mismo, de su derecho a la asesoría legal sobre cómo le puede afectar la IA y a los recursos pertinentes contra los resultados de IA empleados por el juez, y en control de sus elecciones, manteniendo la posibilidad de apartarse del uso del sistema de IA. El usuario debe estar también claramente informado de cualquier procesamiento previo de un caso por inteligencia artificial antes o durante un proceso judicial y tener derecho a objetar, de modo que su caso pueda ser escuchado directamente por un tribunal en el sentido del artículo 6 del CEDH. Tanto jueces como usuarios-administrados pueden poder revisar los resultados arrojados por la IA y continuar el proceso sin ellos y sin estar obligados a hacerles caso. También debe haber Instrucciones de alfabetización informática sobre la IA para los usuarios.

El *Libro Blanco sobre la IA* mostraba una doble preocupación: promover el empleo de la IA y establecer unas garantías o cautelas para proteger los derechos fundamentales de los ciudadanos en su uso. A esta segunda se ha dedicado el proyecto de Reglamento sobre IA de la UE, que, en palabras de De Miguel Asensio, trata de «dar una respuesta proporcional al riesgo generado por los sistemas de IA»[62].

Respecto al principio de respeto de los derechos fundamentales, los derechos que podrían socavarse mediante el empleo de IA en los procesos judiciales son los relacionados con el art. 6 CEDH, esto es, el derecho a un proceso equitativo, lo que en el Derecho español denominamos el derecho a la tutela judicial efectiva, y que engloba derechos más concretos como el derecho de acceso al juez y al recurso frente a sus decisiones; el derecho a un juicio justo, el derecho a la no discriminación, el derecho a un juez independiente e imparcial, presunción de inocencia, el principio de contradicción (o derecho de audiencia defensa) e igualdad procesal, e incluso el derecho a disponer de tiempo suficiente para preparar su defensa). Resulta fácil poner ejemplos en que algunos de estos derechos podrían ser vulnerados por el uso, por parte del juez, de sistemas de IA.

Lo lógico es que los sistemas de IA que se usen durante el proceso hayan sido diseñados de forma ética y con respeto a los derechos humanos (*ethical-by-design*/*human rights-by-design*), pues el diseño del algoritmo es esencial para que el juez no tenga que corregir las desviaciones que el sistema podría generar, que se traducirían automáticamente en vulneraciones de los derechos fundamentales. En España, el Comité Técnico Estatal de la Administración Judicial Electrónica, del CGPJ, debería realizar la labor de conversar con las empresas punteras del sector para la compra de sistemas así elaborados para su posterior empleo en el sistema judicial nacional.

Un gran problema, difícil de resolver, lo tenemos en la prevención de la discriminación de los individuos o grupos de individuos. El dilema aquí es si usar lo que la doctrina llama "datos sucios" o no, es decir, datos personales que si bien no determinan la culpabilidad de la comisión de una infracción penal o administrativa o de su posible reincidencia (algo que, en el procedimiento administrativo sancionador y en el contencioso puede suponer la adopción de medidas cautelares o no contra el supuesto infractor) sí pueden dar indicios al juzgador o elementos de juicio para facilitarle el proceso intelectivo de atribución de la culpa, como los datos referentes a su nacionalidad, religión, creencias políticas, datos genéticos y biométricos, datos de su salud, indicadores socioeconómicos, vida sexual u orientación sexual, etc. Porque si partimos de datos completamente limpios o desnudos, será imposible establecer un perfilado o *profiling* de

61. A este derecho se le conoce también como principio de lealtad digital.

62. Cfr. De Miguel Asensio 2023, p. 121.

la persona acusada, impidiendo a la IA la ayuda al juzgador. Imaginemos un profesor que, en la Universidad, acosa sexualmente a un alumno. Su orientación sexual puede ser un indicio de su culpabilidad, y, respecto a su posibilidad de reincidencia con otros alumnos, su perfil de acosador en serie podría determinar que se adoptara una medida de suspensión de sueldo y empleo mientras se instruye el procedimiento sancionador interno y luego en el juicio penal. Aquí tenemos el eterno debate entre eficacia (mediante el uso de estos datos sensible) o el de protección de la intimidad y pérdida de dicha eficacia[63]. Desde luego, los procesos penales y contencioso-administrativos en materia de infracciones tienen que resolverse conforme a la técnica de individualización de las sanciones, siendo las herramientas de IA sólo colaboradoras de la decisión de concreción de las penas o de las medidas cautelares, ya que éstas suelen arrojar resultados deterministas que pueden no casar con el asunto concreto que está *sub iudice*.

Las herramientas de IA están siendo usadas, sobre todo, por las empresas privadas (bufetes de abogados, compañías de seguros, la banca para estudiar el riesgo del crédito – calificados de alto riesgo en el proyecto de Reglamento europeo de IA –, servicios legales, inversores en bolsa para apostar por determinados valores, etc.), porque buscan reducir la incertidumbre de las decisiones administrativas y judiciales. En Europa, por ahora, los jueces no las están empleando, aunque sabemos que las empresas privadas diseñadoras y comercializadoras de estos sistemas de IA están presionando a los funcionarios encargados de tramitar y resolver procedimientos administrativos y a los jueces-magistrados del sistema judicial de muchos países occidentales para que comiencen a usarlas y se hagan adictos a ellas[64].

Se trata de sistemas de justicia predictiva que procesan *big data* de la jurisprudencia, para ofrecer la *ratio decidendi* de un caso similar[65]. Esos sistemas, cada vez mejores, pueden añadir datos de doctrina legal y de doctrina académica. Esto puede suponer un avance a la hora de darle coherencia

63. La Carta Ética Europea lo expresa así: «La disponibilidad de datos es una condición esencial para el desarrollo de IA, lo que le permite realizar ciertas tareas previamente realizadas por humanos de manera no automatizada. Cuantos más datos estén disponibles, más IA podrá refinar modelos mejorando su capacidad predictiva. Por lo tanto, un enfoque de datos abiertos para las decisiones judiciales es un requisito previo para el trabajo de las empresas de tecnología legal especializadas en motores de búsqueda o análisis de tendencias». El problema, claro está, de los datos abiertos y de la *big data* es la vulneración de los derechos de los ciudadanos. Desde luego, abogamos por la no inclusión de datos privados en el *open data*, es decir, en las bases de datos de jurisprudencia o de doctrina legal. Esos datos deben ser, por tanto, anonimizados o seudonimizados. Lo mismo debería ocurrir en los actos administrativos. Las autoridades nacionales deberían borrar o seudonimizar los nombres, direcciones, números de teléfono, cuentas bancarias, impuestos, estado de salud, etc., en resumen, datos del art. 6 del Convenio 108 del Consejo de Europa (Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal) y del art. 9.1 del RGPD. Todas las resoluciones judiciales de un Estado deberían ofrecerse en abierto, ciertamente (open data) y no sólo la de sus Tribunales superiores (jurisprudencia), pero sin esos datos sensibles. Y sobre esos datos actuarían los sistemas de IA. A nivel interno, de uso profesional por parte de los jueces de un determinado sistema de IA, sí podrían incluirse datos como la reincidencia de un delincuente, los años de su condena, las circunstancias del caso, etc., porque son datos objetivos que sí tienen que ver con la conducta del reo, y no accesorios o sucios. Lo mismo en el contencioso-administrativo en materia de infracciones y sanciones.

64. Evidentemente, no. Es lo mismo un sistema de IA generativa, de perfilado o de análisis predictivo que otro que ayude a redactar la propuesta, buscadores de jurisprudencia y doctrina, resolución de disputas online (intra o extraprocesalmente), de clasificación de contratos según su objeto o *chatbots* de ayuda a los litigantes. La Carta ética arriba citada menciona algunos sistemas secundarios en Europa como Doctrine.fr, Prédictice, Jurisdata, Luminancia, Watson/Ross, Ciervo o Lex Machina.

65. Cfr. Salom Lucas 2021, p. 50 propone, para mejorar las búsquedas de jurisprudencia en el ámbito judicial, superar la búsqueda según el álgebra de Boole (búsquedas booleanas) y pasar a sistemas de búsqueda conceptual, con asistencia del sistema a la hora de introducir la pregunta, con feedback y con capacidad para buscar la mejor jurisprudencia según el *petitum* de la demanda.

a la jurisprudencia[66] (para casos similares, algo muy caro al *due process of law* anglosajón), pero un hándicap en lo que puede suponer que el juez, por pereza o por presión de trabajo, acabe validando los resultados de la IA, que pueden partir de datos imprecisos o tener sesgos o carencias. Y ahí vendría la afectación de los derechos de los administrados, por una especie de "tiranía del algoritmo".

Principios como la primacía de la ley podrían verse sustituidos por la dictadura de la lógica de las máquinas; el estado de derecho, el *iura novit curia*, el derecho a la igualdad, etc. podrían verse afectados cuando la resolución ofrecida por la IA tiene fallos, errores o desviaciones. Y, sobre todo, ¿se apartará el Juez, tan presionado por el tiempo de resolución, de las soluciones ofertadas por la IA, haciéndose responsable de ese apartamiento ante los administrados? ¿Se leerá y revisará todas las resoluciones ofrecidas por la máquina? Soy bastante pesimista al respecto. Estas carencias, omisiones y dejación del deber de cuidado en un tema tan esencial como la justicia pueden tener un mayor impacto en los juicios penales y contencioso-administrativos, por la importancia de los bienes en juego. Mucho me temo que, poco a poco, cuando el sistema judicial arroje datos que muestran cómo la inmensa mayoría de las resoluciones judiciales son las ofrecidas por la IA, acabemos pasando a sustituir los jueces personales por jueces robot, con el enorme peligro que eso encierra, no sólo porque esas resoluciones estarán predeterminadas por un puñado de grupos empresariales que tienen capacidad de diseñar este tipo de algoritmos complejos y de influir en su lógica (basta jugar un rato con Chatgpt para ser muy conscientes de su sesgo *woke*[67]) sino porque siempre va a existir un buen porcentaje de casos resueltos injustamente, algo que el juez-persona sí podría detectar.

Dicho lo cual, no debemos tampoco asombrarnos de un hecho cierto: muchos jueces y tribunales usan resoluciones tipo (ajenas o suyas) anteriores para motivar la sentencia, arrastrando las mismas razones para justificar la resolución de casos similares. En esa labor de producir resultados iguales para casos idénticos, la IA no causaría mayor problema, siempre que haya una final comprobación por el juez. Lo que nunca debería hacer la máquina es una propuesta de resolución creativa, pues ahí la motivación sería ciertamente difícil de comprender y de aprobar por parte del juez[68].

6. El empleo de la IA en los sistemas judiciales en los proyectos de reglamento IA de la UE y de convenio marco de IA del Consejo de Europa. El límite del respeto de los derechos fundamentales

El proyecto de Reglamento Europeo sobre Inteligencia artificial[69] parte de la premisa de que su uso

66. En USA existen las *sentencing guidelines*, destinadas a lograr cierta uniformidad en las decisiones judiciales. Se iniciaron de forma voluntaria por jueces de Denver y Vermont, para ir luego siendo aceptadas por Estados como Maryland, Florida, Massachussetts, Michigan, New Jersey, Utah y Wisconsin. Se trata de configurar unos criterios que permitieran eliminar la disparidad de las condenas: reglas numéricas orientadoras y voluntarias, que exigieran una motivación en caso de separación. Esas guidelines pueden aplicarse mediante IA. Cfr. Barona Vilar 2021, p. 630.
67. Lo que yo llamo el "Google state of mind". Los sesgos algorítmicos pueden ser de dos tipos: imputación de consecuencias judiciales a personas que no están directamente ligados a los hechos o a datos que estén a su vez directamente relacionados con su actuación y, por otro, el ocultamiento de datos reales que pueden ser relevantes para el juicio, por ser políticamente incorrectos. Desde luego, Chatgpt y otras IA generativas incurren sistemáticamente en este segundo, y podrían acabar contaminando al juez si lo usa para instruirse de la parte técnica de un asunto que está juzgando. Podría ocurrir que, a nivel judicial, se den ambos. En el primer caso el algoritmo puede discriminar al individuo y estigmatizarle preventivamente al margen de su conducta. En el segundo se omite u oculta la verdad completa del mismo, con la excusa de que no tiene nada que ver con la resolución del asunto.
68. Cfr. Vélez-Quinteros 2023, pp. 224-225, los sistemas de IA se nutren de datos de casos pasados, y eso puede provocar también una especie de "petrificación" de la motivación, algo que no ocurriría con la supervisión del juez, que usa siempre elementos fácticos nuevos para añadir matices a los precedentes.
69. Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, Bruselas, 21.4.2021, COM(2021) 206 final.

en el ámbito de la justicia es positivo. Lo confirma su Considerando 3°, que dice así: «La inteligencia artificial es un conjunto de tecnologías de rápida evolución que puede generar un amplio abanico de beneficios económicos y sociales en todos los sectores y actividades sociales. El uso de la inteligencia artificial puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la educación y la formación, la administración de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, y la mitigación del cambio climático y la adaptación a él, entre otros, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones.»[70].

Parece que aquí la UE está pensando en las ventajas sociales de una más rápida resolución de los pleitos, de un ahorro de tiempo y de papel, que puede tener beneficios sociales y ambientales, al tiempo que proporcionar un nicho de mercado para las empresas del sector.

Pero en el Considerando 40 se clasifica algunos sistemas de IA en materia de administración de justicia como "de alto riesgo", es decir, muy peligrosos: «Deben considerarse de alto riesgo ciertos sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede considerar de alto riesgo aquellos sistemas de IA cuyo objetivo es ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. No obstante, dicha clasificación no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia en casos concretos, como la anonimización o seudonimización de las resoluciones judiciales, documentos o datos; la comunicación entre los miembros del personal; tareas administrativas, o la asignación de recursos.»[71].

En el Anexo III, apdo. 8. A) de la propuesta de Reglamento se incluyen expresamente: «sistemas de IA destinados a ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos.»

Nótese que el Reglamento IA de la UE sólo califica como de alto riesgo los sistemas de ayuda al Juez en su labor de investigación, interpretación de hechos (prueba) y de la Ley (bases de datos), así como en la aplicación de la ley a los hechos (labor resolutiva), por lo que no están incluidas en esa calificación las herramientas de IA de organización de la justicia, asignación de recursos o actividades administrativas accesorias (IA de gestión), como la anonimización de las resoluciones judiciales, la comunicaciones internas, recursos informáticos y expedientes digitales.

El nuevo Considerando 28 *bis*, introducido por el Parlamento, indica que la clasificación de

70. Éste es el texto original. Sin embargo, el Parlamento Europeo introdujo algunas condiciones más en el texto de este Considerando, de forma que esas posibles ventajas quedan condicionadas: «si se desarrolla de conformidad con los principios generales pertinentes con arreglo a la Carta y los valores en los que está fundada la Unión». Y explica cuáles podrían ser esas ventajas: «El uso de la inteligencia artificial, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y de las organizaciones… puede proporcionar ventajas competitivas esenciales a la empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de …».

71. Una enmienda introducida por el Parlamento ha dejado aún más clara la cuestión, pues ha introducido el siguiente párrafo dentro de este Considerando: «La utilización de herramientas de inteligencia artificial puede apoyar la toma de decisiones, pero no debe substituir el poder de toma de decisiones de los jueces o la independencia judicial, puesto que la toma de decisiones finales debe seguir siendo una actividad y una decisión de origen humano». También se incluye ahora en su ámbito objetivo las resoluciones de los órganos administrativos.

un sistema de IA como "de alto riesgo" se hace por su posible afectación a derechos fundamentales[72] (teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca).

El empleo de sistemas de IA no ha sido considerado como de riesgo inadmisible, sino como de alto riesgo. Esto implica una serie de requisitos específicos para ellos, así como obligaciones para los proveedores de tales sistemas. Dichos sistemas de IA tendrán que cumplir una serie de requisitos horizontales obligatorios que garanticen su fiabilidad y ser sometidos a procedimientos de evaluación de la conformidad antes de poder introducirse en el mercado de la Unión. Del mismo modo, se imponen obligaciones previsibles, proporcionadas y claras a los proveedores y los usuarios de dichos sistemas, con el fin de garantizar la seguridad y el respeto de la legislación vigente protegiendo los derechos fundamentales durante todo el ciclo de vida de los sistemas de IA[73].

Los sistemas de IA de alto riesgo están permitidos en el mercado europeo siempre que cumplan determinados requisitos obligatorios y sean sometidos a una evaluación de la conformidad *ex ante*[74].

Los sistemas de IA empleados en la administración de justicia son del tipo "independiente", es decir, sistemas desvinculados de la seguridad de un producto (máquinas, productos sanitarios, juguetes, etc.), y vienen incluidos en el Anexo III de la propuesta de Reglamento.

La lista de sistemas de IA de alto riesgo que figura en el anexo III contiene un número limitado de sistemas de IA cuyos riesgos ya se han materializado o es probable que lo hagan próximamente. La Comisión podría ampliar la lista de sistemas de IA de alto riesgo utilizados.

Los requisitos que se imponen a estos sistemas de IA vienen recogidos en el cap. 2° del Título III se refieren a la calidad de los datos empleados y su gobernanza, la documentación y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la seguridad. Y en el cap. 3° se integran los requisitos horizontales a imponer a las empresas proveedoras de estos sistemas.

Estas empresas deben realizar una evaluación integral de la conformidad *ex ante* mediante controles internos, combinada con una supervisión *ex post* estricta, y luego deben inscribir sus aplicaciones o sistemas en el registro europeo, de modo que las Administraciones públicas se encarguen luego de su revisión periódica. Todo esto se integra en un sistema de gestión de riesgos asociado a cada

72. «A la hora de clasificar un sistema de IA como de alto riesgo resulta particularmente pertinente atender a la magnitud de las consecuencias adversas de dicho sistema de IA para los derechos fundamentales protegidos por la Carta. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración».

73. A los proveedores de sistemas de IA de alto riesgo de les imponen requisitos relativos a la alta calidad de los datos, la documentación y la trazabilidad, la transparencia, la vigilancia humana, la precisión y la solidez son estrictamente necesarios para reducir los riesgos de la IA para los derechos fundamentales y la seguridad y que no están cubiertos por otros marcos jurídicos existentes. La Comisión viene obligada a establecer un Registro de aplicaciones de IA de alto riesgo independientes, en una base de datos pública para toda la UE. Este Registro también permitirá que las autoridades competentes, los usuarios y otras personas interesadas verifiquen si un sistema de IA de alto riesgo cumple los requisitos estipulados en la propuesta y ejerzan una vigilancia reforzada de aquellos sistemas de IA que entrañan un alto riesgo para los derechos fundamentales. Para alimentar esta base de datos, los proveedores de IA estarán obligados a facilitar información significativa sobre sus sistemas y la evaluación de la conformidad a la que los sometan.

74. Como dice el art. 9.7 de la propuesta de Reglamento, los sistemas de alto riesgo se realizarán antes de su introducción en el mercado o puesta en servicio. Los ensayos se realizarán a partir de parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista *o el uso indebido razonablemente previsible* del sistema de IA de alto riesgo de que se trate.

sistema de IA de alto riesgo, que pervivirá durante todo el ciclo de vida de dicho sistema de IA (art. 9).

El empleo de sistemas de IA en la administración de justicia puede ser propenso a afectar a colectivos vulnerables, por sus sesgos de origen, no siempre fácilmente identificables, a pesar de que se diseñen desde su origen de forma que sean lo más neutrales posibles. Por eso el art. 9.8 de la propuesta de Reglamento exige *que los proveedores presten* especial atención a la probabilidad de que *grupos vulnerables de personas* o menores *se vean afectados negativamente por el* sistema de IA de alto riesgo de que se trate.

En resumen, la UE viene a clasificar como de alto riesgo los sistemas de IA fuertes, generativos o de *deep learning*, dirigidos a dar soluciones acabadas a un caso concreto, mediante la investigación e interpretación de los hechos y del derecho aplicable, pero no generan riesgos los que son de simple apoyo al juez para tomar sus decisiones, ya sean basados en bases de datos como en procesos de gestión.

Se acusa a la UE que ha decidido aprobar un Reglamento sobre la base de su competencia en materia de seguridad de los productos[75] cuando, ciertamente, es la única que le podría dar margen competencial para regularla. Eso implica que conforme al principio de mínima intervención y al de precaución, se trata de preceptos que tienen a permitir el empleo de la IA, con una serie de requisitos proporcionales al posible daño que los distintos sistemas de IA pueden ocasionar. Es, por tanto, un enfoque mínimo, teniendo en cuenta la materia de mercado y de productos que la sostiene.

A ese enfoque debemos sumar el que hace el Consejo de Europa, no ya sólo con su Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno, que ya hemos comentado, sino también con el Convenio que ahora mismo se está negociando en el Consejo de Europa sobre Inteligencia artificial, derechos humanos, democracia y Estado de Derecho, titulado "Convenio Marco sobre el Desarrollo, Diseño y Aplicación de sistemas de IA basados en los estándares del Consejo de Europa sobre derechos humanos, democracia y estado de derecho"[76]. Si el Reglamento europeo de IA va destinado a proveedores y usuarios de estas herramientas, el Convenio lo está a los Estados partes del Tratado (la UE entre ellos). Si aquél se fundamenta en los riesgos que el software de IA puede ocasionar en los ciudadanos, éste se basa en el respeto de los derechos del CEDH. Si aquél presta mucha atención a los sistemas de IA de alto riesgo, éste no presta esa atención específica. Finalmente, si aquél impone una serie de requisitos *ex ante* a las empresas productoras de sistemas IA (evaluación de conformidad, evaluación del impacto en los derechos fundamentales) y requisitos horizontales *ex post*, éste establecerá unos requisitos ex ante sobre la evaluación de los riesgos y sus efectos, y límites para que no se vulneren derechos y garantías procesales.

En relación con las medidas que el Convenio Marco del Consejo de Europa sobre IA establece en materia de aplicación de sistemas de IA al ámbito judicial habría que comenzar diciendo que, como es propio del margen de actuación que la jurisprudencia del TEDH otorga a los Estados para establecer el estándar adecuado de protección, también aquí, en su art. 2, se establece que cada Estado mantendrá y adoptará en su ordenamiento jurídico interno las medidas graduadas y diferenciadas que sean necesarias y apropiadas en vista de la gravedad y probabilidad de ocurrencia del impacto de estos sistemas en los derechos humanos y las libertades fundamentales, la democracia y el Estado de derecho durante el diseño, desarrollo, uso y desmantelamiento de sistemas de inteligencia artificial[77].

75. La base jurídica de la propuesta es, en primer lugar, el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que trata de la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior que deriva, a su vez, de la competencia exclusiva de la UE sobre la política comercial común (art. 3.1, e TFUE) y de la competencia compartida sobre mercado interior del art. 4.2, a TFUE.

76. Publicado su borrador inicial el 6 de enero de 2023 y su Borrador revisado el 7 de julio del mismo año. Puede consultarse aquí: https://www.coe.int/en/web/artificial-intelligence/cai.

77. En particular, se ha de velar por la transparencia en el diseño del algoritmo, su desarrollo, uso y desmantelamiento de los sistemas de IA, con un trámite de información pública (art. 19); en la responsabilidad e imputabilidad de daños a los fabricantes de los mismos; en la igualdad y no discriminación durante su empleo; en la privacidad y protección de los datos personales; en la seguridad, Seguridad, protección y robustez de los datos empleados.

La definición que hace de IA es amplia (no puede ser de otra forma) y engloba los dos tipos de actuaciones que estas herramientas pueden jugar en el ámbito judicial: asistente del juez o reemplazo del mismo[78].

La razón de ser del Convenio es la protección de la dignidad humana, autonomía individual, derechos humanos, libertades fundamentales, democracia y estado de Derecho, en positivo, mientras que esos mismos derechos fundamentales actúan como límite negativo en los sistemas declarados de alto riesgo en la propuesta de Reglamento IA de la Unión Europea.

El art. 6 del Convenio Marco nos parece muy relevante porque condena los sesgos ideológicos que tienen muchos sistemas de IA. Muchas personas hemos advertido de que *chatgpt* tiene un clarísimo sesgo *woke*, que puede acabar influyendo en la libertad de toma de decisiones de los que los usan. Y otros sistemas de IA pueden incidir en la libertad de criterio de los operadores jurídicos, incluso de los jueces. Y en su apdo. 2° aconseja a cada Estado a que tome las medidas necesarias para garantizar que los sistemas de inteligencia artificial no se utilicen para socavar la integridad, la independencia y la eficacia de las instituciones y procesos democráticos, incluido el respeto a la independencia judicial y el principio de separación de poderes. Aquí podemos reproducir las reflexiones que hicimos arriba sobre cómo los sistemas de perfilado o de jurimetría pueden acabar afectando a la imparcialidad e independencia judicial. Y, por supuesto, este límite prohibiría que las decisiones judiciales pudieran ser adoptadas en exclusiva por estos sistemas computacionales.

Igualmente relevante para el empleo de la IA en el sistema judicial es su art. 14.1, que exige que cuando un sistema de inteligencia artificial informe sustancialmente o tome decisiones que impacten [potencialmente] en los derechos humanos y las libertades fundamentales, deban existir garantías procesales, salvaguardias y derechos efectivos, de conformidad con el derecho interno e internacional aplicable, disponibles para cualquier persona afectada por el mismo. Esto reclama, claro está, el derecho a exigir que una resolución procesal se tome por parte del juez y si existiera un sistema de IA de carácter asistencial, se le informe de su funcionamiento y de su ley interna, en términos que él pueda comprender. También del derecho al recurso frente a la decisión informada o adoptada por una herramienta de IA, que debería darse siempre, habida cuenta de que la motivación del recurso se refiere al empleo de la IA y no al fondo del asunto, aunque esa resolución judicial no reconozca la existencia de un recurso.

El art. 15 del Convenio Marco, en realidad, es una reproducción del enfoque preventivo de la propuesta de Reglamento IA de la UE, así que no incidiremos más en él.

7. Algunas especificidades del empleo de la IA en el orden contencioso-administrativo

7.1. Si ya cabe el dictado de actos administrativos automatizados, ¿podría ocurrir lo mismo en la resolución de juicios contencioso-administrativos?

Al igual que la actuación administrativa automatizada de los arts. 41 y ss. de la Ley 40/2015 (LRJSP) se usa principalmente para el dictado de actos administrativos electrónicos derivados de potestades administrativas regladas, declaraciones responsables o comunicaciones previas, en el ámbito procesal contencioso-administrativo la IA debería jugar un papel subalterno de ayuda al juez, y, como mucho, sólo podría comportarse de forma decisoria en juicios simples. Nótese que el art. 41 de dicha Ley no establece límites objetivos a esa automatización, pudiendo automatizarse "cualquier acto o actuación" de una "Administración Pública en el marco de un procedimiento administrativo", cabiendo entonces actos-resolución, actos de trámite, actos de impulso y de instrucción, etc., pero todos ellos deberían venir firmados por la persona responsable. Es decir, el contenido del acto,

78. Art. 3: «se entiende por "sistema de inteligencia artificial" cualquier sistema algorítmico o una combinación de tales sistemas que utilice métodos computacionales derivados de estadísticas u otras técnicas matemáticas y que genere texto, sonido, imagen u otro contenido que ayude o reemplace a los seres humanos».

debidamente informatizado[79], podría generarlo la IA, pero siempre debe ser debidamente firmado, de forma que el titular competente para su dictado es quien dicta el acto.

Los dos requisitos que establece el art. 41.2 de la LRJSP son, en primer lugar, la previa determinación del órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Y, en segundo, la concreción del órgano que debe ser considerado responsable a efectos de impugnación. Entendemos que, por analogía, ambos requisitos son también aplicables al ámbito judicial, algo que quedó ratificado por el art. 42 de la Ley 18/2011, de 5 de julio, Reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, que, al no poder prever el uso de sistemas de IA, se limitó a regular la digitalización y automatización de la administración de justicia, de forma que, en clara sintonía con la LRJSP, venía a exigir que, en caso de actuación automatizada, deberá establecerse previamente por el Comité Técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso la auditoría del sistema de información y de su código fuente. Será, pues, este Comité Técnico el que debe aprobar los sistemas de justicia automatizada, dentro del marco establecido por el CGPJ. Y el que debería crear un sistema de formación o entrenamiento de los jueces al respecto[80].

Por tanto, si ya se dictan actos administrativos automatizados, como la imposición de multas de tráfico por radar, al tratarse de un valor parametrizable, en teoría podría ocurrir lo mismo en la vía judicial contenciosa. Pero no parece fácil poder permitirlo, desde el momento en que los actos administrativos dictados completamente por máquinas o automatizados nunca podrían ser resoluciones de recursos administrativos, como se desprende del art. 41.2, *in fine* LRJSP. Los actos de juicio, por tanto, parecen estar excluidos de su resolución automatizada.

En el caso en que se quiera revisar ante la jurisdicción contencioso-administrativa un acto administrativo para cuyo dictado se ha empleado técnicas de IA (por ejemplo, en la delimitación e investigación de bienes de dominio público, en el otorgamiento de subvenciones, en la selección de personal de la Administración, o en los entes locales, entre otros…) a juicio de Berning sería necesaria una pericial que permitiera saber al juez cómo funcionan esos algoritmos[81], ya que, por motivos de propiedad intelectual, es muy probable que no se permita a la parte demandante conocer cómo funciona[82].

7.2. ¿Es apto el orden jurisdiccional contencioso-administrativo para el empleo de sistemas de IA?

El empleo de la IA en el ámbito de la administración de justicia está suponiendo una revolución,

79. Parece razonable su empleo en la respuesta administrativa a declaraciones responsables o comunicaciones previas, en los que la previa presentación, por el administrado, de la documentación en el registro electrónico puede usarse para producir el acto administrativo automatizado.

80. El art. 16 del Borrador del Convenio Marco del Consejo de Europa sobre IA considera que ese entrenamiento debería dirigirse a todos los que vayan a usar un sistema de IA que pueda potencialmente afectar a los derechos fundamentales. Incluso a todos los segmentos de población, como una enseñanza transversal (art. 20).

81. En Holanda, Austria o Italia ya han sido anulados actos administrativos basados en el empleo de sistemas de IA por insuficiente motivación de los mismos. El Tribunal de Distrito de La Haya pronunció una sentencia el 5 de febrero de 2020, mediante la que anuló una elaboración de perfiles para la lucha contra el fraude, implantada por el Gobierno holandés, que únicamente se utilizó en los calificados como "vecindarios problemáticos", concluyendo el Tribunal que ese criterio puede provocar exclusión, discriminación y estigmatización injustificadas. Desde 2013, 26.000 familias fueron injustamente acusadas de fraude y obligadas a devolver las subvenciones que recibieron. Este escándalo acabó forzando nuevas elecciones en Holanda. Cfr. Gamero Casado 2023, p. 423.

82. Cfr. Berning-Prieto 2023, pp. 121-122.

sobre todo en la jurisdicción penal: predictibilidad, prevención, investigación, fundamento de las decisiones judiciales[83]… a través de herramientas de IA están aumentando exponencialmente su empleo, de una forma informal o alegal.

Sin embargo, el hecho de que el proceso contencioso-administrativo sea esencialmente escrito (a diferencia del penal o del civil) le haría potencialmente apto para el empleo de sistemas de IA, ya que éstos se basan en datos y la escritura facilita el empleo de sistemas computacionales. En el contencioso las vistas orales son escasas pero en esos casos también sería posible el empleo de herramientas de IA de traducción automática en tiempo real de otros idiomas al español, sin necesidad de intérprete. O, al menos el intérprete jurado debería confirmar los elementos esenciales de las declaraciones, no toda la declaración realizada por la parte extranjera.

En los procesos civiles, mercantiles, penales y laborales ambas partes parten de una posición de igualdad, más allá de las diferentes posiciones de las partes enfrentadas. Pero en el contencioso-administrativo la presunción de veracidad del acto administrativo y el impacto del ejercicio de las potestades administrativas, especialmente de las discrecionales o de la interpretación de los conceptos jurídicos indeterminados[84] y de las cláusulas contractuales, de forma unilateral, por parte de la Administración, añaden un plus de peligrosidad al empleo de sistemas de inteligencia artificial en dicho orden jurisdiccional[85].

Al contencioso-administrativo en materia de infracciones se pueden aplicar todos los sistemas de IA y, a la vez, todas las limitaciones en defensa de los derechos fundamentales que se suscitan en el proceso penal: así, la identificación de personas mediante datos biométricos, prohibida en el art. 9 RGPD pero con excepciones que permitirían su uso limitado en el proceso, como por ejemplo que el usuario haya difundido públicamente esos datos, verbigracia, en redes sociales de libre acceso[86].

Evidentemente, el empleo de sistemas de IA en la administración de justicia requiere un cambio en la legislación procesal. Básicamente en la LOPJ, siendo la competencia exclusiva del Estado (art. 149.1, 6ª CE). Debería incluir el posible empleo de IA, con las condiciones mínimas que impondrá el Reglamento de IA de la UE y los que el Estado español quiera añadir: bien podría materializarse en sendas modificaciones de la LOPJ, la LJCA y la LEC. Esa regulación debe establecer el marco jurídico del uso de la IA aplicada en los procesos judiciales y, especialmente, en el orden contencioso-administrativo y de las garantías necesarias para el respeto de los derechos fundamentales de la parte demandante y de las personas que en ellos participen. El CGPJ debe ocuparse de la seguridad de estos sistemas que, hasta ahora funcionan en la alegalidad o, como dicen los alemanes, en la cara oculta de la Luna, *die dunkle Seite des Mondes* (su uso privado por parte de los jueces de manera informal). Mejor regular que dejarla a su empleo libre y secreto por parte de los jueces.

La actividad judicial automatizada debería quedar limitada, pues, a los actos de impulso e instrucción del proceso contencioso, plazos, notificaciones, registros, acuses de recibo, y otros actos sin contenido material. La resolución por IA del proceso es harina de otro costal.

83. Cfr. Barona Vilar 2021, p. 346.

84. Cfr. Gil Cruz 2021, p. 33.

85. Lo mismo ocurriría en el proceso penal (o en el contencioso-administrativo) en materia de infracciones y sanciones, en el que la parte acusadora-sancionadora podría situarse en una posición de superioridad sobre la parte acusada como consecuencia del empleo de sistemas de IA, a la que no tiene acceso ésta última. Cfr. Ponce Solé 2019, p. 21, se muestra contrario al empleo de IA para el ejercicio de potestades administrativas.

86. En el proyecto de Reglamento de IA de la UE se define la identificación biométrica como «La noción de "identificación biométrica" tal como se utiliza en el presente Reglamento debe definirse como el reconocimiento automatizado de rasgos físicos, fisiológicos, conductuales y psicológicos humanos, como la cara, el movimiento ocular, las expresiones faciales, la forma del cuerpo, la voz, el habla, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el dolor, las pulsaciones de tecla, las reacciones psicológicas (ira, angustia, dolor, etc.) a efectos del establecimiento de la identidad de una persona mediante la comparación de los datos biométricos de esa persona con datos biométricos de personas almacenados en una base de datos (identificación mediante comparación "uno respecto a muchos")».

Dentro de los sistemas de justicia automatizada se podría incluir determinado *software* de inteligencia artificial, tanto bases de datos de jurisprudencia, doctrina, etc. como la posibilidad que se puede dar al juez o magistrado de elegir entre varias opciones de resolución predeterminadas (sistemas expertos)[87]. Como se ve, se trata de sistemas de IA de ayuda, que dejan en manos de la persona del juez o magistrado la decisión final.

Ha sido Chaves García quien ha propuesto que que puedan llegar a articularse procedimientos judiciales abreviados contencioso-administrativos por medios completa y exclusivamente electrónicos de IA, cuando nos encontremos ante circunstancias determinadas de casos sencillos, o determinados casos de ejecución de sentencias[88].

La clave aquí, como venimos diciendo, sería salvaguardar las garantías procesales y la tutela judicial efectiva, mediante fórmulas que permitan el control de estos sistemas de IA por parte del CGPJ.

Para Martínez Gutiérrez, sería posible "parametrizar" o baremar las soluciones judiciales aplicables sobre la base de la doctrina jurisprudencial consolidada de lo contencioso-administrativo, en una suerte de justicia predictiva. El problema, ya lo vimos antes, es el del sesgo de los algoritmos y su opacidad a la hora de que el operador jurídico pueda revisar cómo se han obtenido los resultados ofrecidos, con el miedo siempre pendiente de que el sistema haya obviado determinadas soluciones, por omitir determinadas sentencias. Puede darse el caso, además, de que el sistema de IA use los datos personales del caso para inducir reglas o parámetros falsos o artificiosos, en lugar de la verdadera *ratio decidendi* del asunto. Con el riesgo añadido de que el juez se inhiba de revisar los resultados, para ganar tiempo, de modo que los algoritmos se acaben comportando como un *Deus ex machina*.

Para evitarlo, tanto el RGPD europeo como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales hablan de privacidad de los sistemas desde el diseño (*privacy by design*). También ha recogido esa exigencia el art. 9.4, a) de la propuesta de Reglamento sobre IA de la UE, que exige eliminar o reducir los riesgos *detectados* en la medida en que sea tecnológicamente factible mediante un diseño y un desarrollo adecuados del sistema de IA de alto riesgo, con la participación, cuando proceda, de expertos y partes interesadas externas.

Está por ver si esas ayudas al juez, con la subsiguiente reducción de tiempos que apunta, aconsejaría la transformación del proceso y de su estructura sobre la base de la actuación de las herramientas de IA, simplificándose y adaptándose a los nuevos modelos computacionales. Es posible que, como nos cuenta Barona Vilar, esto pueda ser así en procesos civiles de escasa cuantía, como ocurre en Estonia (hasta 7.000 euros)[89]. Y podríamos añadir nosotros que, por analogía, tal podría ser el caso de procesos contencioso-administrativos en los que la cuantía sea igualmente pequeña, en asuntos de infracciones, multas, reclamaciones de responsabilidad menores, ejecución forzosa de actos administrativos, subvenciones y ayudas. También podría ser campo abonado para la propuesta de resolución mediante IA los procesos de caso testigo, recogido en los arts. 37.2 y 3 y 111 LJCA.

Los sistemas jurídicos expertos analizan los ingentes datos de la jurisprudencia, la legislación, la doctrina legal e incluso la doctrina académica para dar conclusiones o patrones y dar soluciones a un problema práctico. Pueden usar mecanismos de silogismos, casos previamente resueltos, aplicación de la analogía, la jurisprudencia, la doctrina académica, la teoría general del Derecho, etc. A veces usan todos ellos a la vez, y son los sistemas más avanzados. Hasta ahora se usan más en casos penales, pero también civiles (asuntos de familia, divorcios, patria potestad o herencias), donde suele existir menos complejidad de matices que en el contencioso-administrativo.

Además, estos sistemas pueden no estar preparados para interpretar adecuadamente los *conceptos jurídicos indeterminados* (imaginemos, por ejemplo, la "equidad" en la revisión de oficio o en la revocación) y escoger entre todas las opciones posibles de una *potestad administrativa discrecional* la mejor para el caso concreto. En estos casos de discrecionalidad, además, sería necesario que

87. Cfr. Martínez Gutiérrez 2019, p. 237.

88. Vid. Chaves García 2018.

89. Cfr. Barona Vilar 2021, pp. 394-395.

una Ley le permitiera a la IA poder tomar decisiones, algo que aún no tenemos, y que tampoco parece aconsejable. Estas incertidumbres, que pueden ser reducidas por un jurista o juez experto, no tienen una solución lógica para las máquinas. La complejidad del razonamiento jurídico y judicial no está al alcance de la IA, que sólo funciona por deducciones y lógica matemática. Y por eso nunca cabría ni debería caber un *juez robot*. Sí como una herramienta de ayuda, un elemento de juicio más, más o menos cualificado. La discrecionalidad, además, y su control, requiere cierta empatía en el funcionario y en el juez, respectivamente, una elección entre varias opciones posibles, basadas en hechos, intereses y derechos relevantes, que se concretará según las circunstancias del caso, y que una máquina nunca podrá poseer[90].

Abunda en ello Pérez Daudí, para quien el razonamiento judicial es mucho más complejo que un simple silogismo, centrándose casi siempre en el respeto al precedente[91]. No diríamos nosotros tanto, ya que la vinculación al precedente es el centro gravitacional de la justicia en el mundo anglosajón, mientras que en el mundo jurídico continental lo es la aplicación de la norma, y la valoración de la prueba, que siempre implica un conocimiento heurístico y nunca del todo exacto o replicable, por tanto, muy humano y poco científico o computable[92]. La adecuada motivación, además, es parte esencial del derecho a la tutela judicial efectiva (art. 24 CE), sobre todo cuando el acto administrativo es restrictivo de derechos o resultado de una potestad administrativa discrecional.

El empleo masivo de la IA fuerte o profunda[93], que puedan ofrecer soluciones completas a un caso sin la intervención humana, en el sistema judicial no será posible a medio plazo. Sí lo será el desarrollo de sistemas de IA débiles o de apoyo al juez, como hemos visto. Su desarrollo está justamente comenzando Son demasiados los riesgos y, mucho nos tememos, son más graves y elevados para los derechos u garantías de las personas que participan en el proceso que los beneficios posibles para las partes.

Elementos finos del proceso como la valoración de la prueba[94] o la motivación de una sentencia son algo puramente humano (que exige la

90. Cfr. Roberto Granero 2022, p. 131.

91. Vid. Pérez Daudí 2022.

92. Recordemos que el art. 100.7 de la LJCA establecía el carácter vinculante de las sentencias del TS en casación por interés de ley, pero fue suprimido por la disposición final 3.2 de la Ley Orgánica 7/2015, de 21 de julio, de modificación de la LOPJ. El TC se pronunció a favor de esa vinculancia, en sus SSTC 111/1992 y 37/2012, entre otras. Pero ha sido decisión política la de anular tal vinculatoriedad, por considerarla contraria a la división de poderes y a la independencia judicial. Respecto a la vinculación de un Tribunal por sus precedentes propios, el TC aclaró en su STC 176/2005, de 5 de mayo, que un tribunal no está vinculado por la jurisprudencia de otro Tribunal, pero que, en relación con su propia jurisprudencia anterior, sólo lo está en casos que sean sustancialmente iguales y que el trato desigual se concrete en una quiebra injustificada del criterio mantenido hasta entonces. Con esta doctrina, las propuestas que los sistemas de IA hagan de determinada jurisprudencia aplicable a un caso son lícitas y legítimas, pero deben quedar sometidas a la labor de control y supervisión del juez, que escogerá la línea jurisprudencial que crea mejor se adapta al caso. Otra cosa, claro está, en el valor vinculante de las resoluciones del TC (art. 5.1 LOPJ), que es determinante sobre cómo interpretar la Constitución, de forma que vinculan al resto de jueces y tribunales. Cfr. Pérez Daudí 2022a, pp. 208-209. Por tanto, respecto a la jurisprudencia del TC, los sistemas de IA deben ofrecer la correcta interpretación de la CE a los jueces como algo inexorable de obligado cumplimiento, no como una opción más.

93. Los sistemas de IA débil son aquellos diseñados para ayudar al usuario a alguna utilidad concreta. Y los sistemas de IA fuerte son multifuncionales y aprenden por sí solos mientras más datos tienen y más se usan, ofreciendo soluciones complejas. Cfr. Barona Vilar 2021, pp. 106-107. Un ejemplo de IA débil, por tanto específica, es el Deep Blue de IBM, que derrotó al ajedrez a Gary Kasparov. A esta doble clasificación se sumaría, en opinión de Barrio Andrés, los sistemas de IA de súper inteligencia, que excedería en razonamiento y capacidad de resolución de problemas a los seres humanos, siendo consciente de su propia "singularidad". Cfr. Barrio Andrés 2020, p. 57. Nosotros creemos, no obstante, que ni las IA fuertes ni las súper inteligentes podrán llegar nunca a la autoconsciencia, sencillamente porque no son seres vivos y carecen de alma.

94. Aunque algún caso existe ya en procesos penales, como el Sistema RYEL, que ayuda al juez a valorar la prueba y a aplicarla al caso mediante grafos e imágenes. Vid. Oconitrillo-Vargas-Burgos-Corchado 2021, pp. 335-343.

ponderación del caso y la aplicación del principio de proporcionalidad), que queda lejos aún de la capacidad real de la inteligencia artificial[95], aunque, como hemos dicho arriba, ciertamente la IA puede ayudar al juez a hacerlo. La labor u oficio del juez (*Judge Craft*) exige comprender las leyes, la jurisprudencia, doctrina académica y doctrina legal, así como debidamente. Pero también concurren emociones, sentimientos, percepciones sensoriales del propio juez, intuiciones, sensibilidades subjetivas, dudas, que, juntas, conforman el pensamiento jurídico judicial[96].

7.3. El posible uso de la IA en algunos trámites del contencioso-administrativo

A. Análisis de la información, para su organización, y evitación de incoherencias

Ciertamente, un sistema de IA que pueda ayudar al juez a resumir o investigar la ingente cantidad de literatura que se produce en el proceso[97], que puede ocupar varios *terabytes* según los casos (IA de análisis de documentación), comenzando por el expediente enviado por la Administración demandada, la demanda y contestación a la demanda realizada, las pruebas producidas y las conclusiones, para así ser más eficiente y poder dedicarle más tiempo a encontrar los argumentos jurídicos (que también podrían ser ofrecidos por otros sistemas de IA) y la *ratio decidendi* de los asuntos.

Aparte del tratamiento, organización y desbroce de los datos contenidos en el expediente, demanda y contestación a la demanda, la IA podría ser empleada, de forma limitada, en los momentos esenciales del proceso contencioso-administrativo.

B. Justicia cautelar

La adopción de medidas cautelares en el contencioso-administrativo está regulada en los arts. 129 y 130 LJCA.

Básicamente, se pueden adoptar las medidas cautelares siempre que su finalidad sea asegurar la efectividad de la sentencia que haya de recaer, y, para ello, el juez debe valorar dos criterios legales (que la ejecución del acto o la aplicación de la disposición pudieran hacer perder su finalidad legítima al recurso; y que no cause perturbación grave de los intereses generales o de tercero) y algunos otros jurisprudenciales, como el *fumus boni iuris* y el *pericumulum in mora*.

De todos ellos, éste último criterio es el más objetivable y, por tanto, susceptible de poder ser informado por los resultados de sistemas de IA. Dejando siempre a salvo la potestad libérrima del juez de ponderar todos los intereses en conflicto, parece evidente que en todas las cuestiones técnicas y científicas que puedan informar el periculum in mora, esto es, la necesidad de adoptar medidas que salvaguarden el objeto del recurso, que podría perderse o ser afectado gravemente sin la adopción de una medida cautelar, algunos sistemas de IA tendrían algo que decir. Por ejemplo, la posibilidad de derrumbe de una casa, la posibilidad de reincidencia de un demandante contra una infracción administrativa de carácter grave, que pudiera afectar a personas; la necesidad de detener los efectos negativos acumulados de un atentado contra algún recurso natural (agua, fauna o flora); la acumulación de construcciones ilegales en una zona no urbanizable, como consecuencia del efecto llamada de una construcción ilegal; el estado de conservación de las obras públicas y su afectación a la seguridad del tráfico, etc. Se trata de herramientas de IA predictivas, donde los algoritmos ofrecen porcentajes de posibilidades sobre la conservación o estado del objeto material del recurso, que ayudarían al juez. Obviamente mucha de esta información se podría obtener también mediante pruebas periciales, a instancia de parte o de oficio, no así las que atienen a la posible reincidencia de un infractor.

C. La prueba

Podría acelerarse el proceso contencioso-administrativo en la fase que más tiempo demanda, la

95. Sí podría tener la IA funciones secundarias en la valoración de la prueba, como la detección de contradicciones en las declaraciones de un testigo, o en el perfilado del perito que puede prestar una pericia (su CV, su calidad, su adecuación para producir el peritaje, su objetividad, etc.) o en la organización de los datos de un reconocimiento judicial. Cfr. Vallespín Pérez 2023a, p. 18.

96. Cfr. Barona Vilar 2022, p. 105.

97. Cfr. Nieva Fenoll 2022, p. 25.

de la prueba, mediante el uso generalizado de la videoconferencia, no sólo para la prueba testifical, sino también para la documental y la pericial, realizándose de forma oral en el mismo día, en aras del principio de concentración y de inmediación.

La STS (Sala de lo penal) de 17 de marzo de 2015, ponente D. Manuel Marchena Gómez, indicó que el uso de la videoconferencia era posible siempre que no se resintieran los principios estructurales de la contradicción y defensa (art. 229 LOPJ). Entendemos que en el contencioso-administrativo su empleo puede ser más amplio y generalizado[98] que en lo penal, ya que la LECrim, en su art. 731 *bis*, exige que su empleo venga demandado por razones añadidas de agilidad, seguridad, orden público, o de constatación de gravamen o perjuicio para el que haya de declarar presencialmente. Habría que superar, claro está, las reticencias de jueces y magistrados, y la jurisprudencia del TC (STC 2/2010, de 11 de enero[99]) y del TEDH.

Es muy posible que se den cada vez más casos en que la inteligencia artificial acabe siendo esencial en la conformación de la prueba misma, pudiendo constituir una fuente de prueba, en todos los órdenes jurisdiccionales: comparando letras, literatura o música, para casos de plagio y propiedad intelectual; manejando y descifrando datos recopilados desde vídeos, fotos, datos de hechos producidos, reconocimiento facial (casos penales o contencioso-administrativos por infracciones); pruebas médicas para casos de responsabilidad patrimonial; o, imaginemos, en casos de resolución técnica (declaración de ruina en urbanismo, por ejemplo), o científica (adn, análisis toxicológicos, balística, análisis de movimientos, etc.) haciendo o elaborando cálculos y estudios que pueden suponer, por sí mismos, una nueva especie de prueba pericial autónoma; o estudios de imágenes por satélite para casos de disciplina urbanística, etc. Son los llamados informes periciales de inteligencia[100]. El problema con ellos es el de la indefensión en la que queda la otra parte, porque es muy difícil oponerse a una prueba realizada mediante sistemas de IA, casi siempre opacos (prueba diabólica). Se hace necesario que esa prueba obtenida mediante IA incluya una explicación comprensible de cómo se han obtenido los resultados ofrecidos. Aquí la labor del juez, validando, refutando o matizando esa prueba es esencial, sino queremos que se produzca un "criterio autosuficiente sobre la fiabilidad de la prueba, reemplazando así el juicio humano"[101].

La tarea de valoración libre, conjunta y racional de toda la prueba lícita practicada, aunque parte de la prueba se haya realizado con sistemas de IA, está sometida a la reserva humana del juez, y, por tanto,

98. La Directiva 2014/41/CE, del Parlamento europeo y del Consejo, de 3 de abril, relativa a la orden europea de investigación en materia penal, favorece en su art. 24 un mayor empleo de la videoconferencia en ese orden jurisdiccional. Tanto más podríamos decir en el contencioso-administrativo.

99. En su Fdto. Jco. 3°, esta STC viene a decir que el uso de la videoconferencia, en aras del principio de inmediación, sólo puede producirse de forma vicarial o subalterna de la comparecencia física, y en casos tasados: «la STEDH de 2 de julio de 2002, caso S.N. c. Suecia, §§ 46, 47, 52 y 53, admite la ausencia de inmediación en relación con procesos penales por delitos sexuales en que resulten afectados menores; y las SSTEDH de 5 de octubre de 2006, caso Viola c. Italia, §§ 67, 70, 72 a 76; y de 27 de noviembre de 2007, caso Zagaría c. Italia, § 29, admiten el uso de la videoconferencia condicionado a que se persigan fines legítimos – tales como 'la defensa del orden público, la prevención del delito, la protección de los derechos a la vida, a la libertad y a la seguridad de los testigos y de las víctimas de los delitos, así como el respeto de la exigencia de plazo razonable' –, y a que su desarrollo respete el derecho de defensa del acusado. En nuestro ordenamiento positivo no faltan supuestos de carencia o defecto de inmediación que no afectan a la validez de la actuación procesal correspondiente (así, en los arts. 306 in fine, 325, 448, 707, 710, 714, 730, 731 *bis* y 777 LECrim) en el bien entendido de que cualquier modo de practicarse las pruebas personales que no consista en la coincidencia material, en el tiempo y en el espacio, de quien declara y quien juzga, no es una forma alternativa de realización de las mismas sobre cuya elección pueda decidir libremente el órgano judicial sino un modo subsidiario de practicar la prueba, cuya procedencia viene supeditada a la concurrencia de causa justificada, legalmente prevista».

100. Cfr. Moreno Catena 2022, p. 67.

101. Cfr. De Hoyos Sancho 2021, pp. 7-8. En definitiva, si no hay suficiente transparencia – acceso al código fuente, *inputs* y *outputs* del *software* – no podrá asegurarse la necesaria y suficiente paridad de armas entre demandante y demandado, el justo equilibrio procesal entre ambas posiciones.

es indelegable. Pero cabría pensar en la posibilidad de emplear IA para la valoración de la coherencia de las pruebas periciales[102].

Y ello, dejando de lado los sistemas de IA encargados de reconocer emociones que pueden ayudar a dar veracidad o no a las pruebas testificales[103], que son aquéllos destinados a detectar o deducir las emociones, los pensamientos, los estados de ánimo o las intenciones de individuos o grupos a partir de sus datos biométricos y sus datos de base biométrica (art. 3, 34 de la propuesta de Reglamento Europeo de IA). El Reglamento ha expresado su preocupación respecto a la base científica de los sistemas de IA que procuran detectar las emociones, los rasgos físicos o psicológicos, como las expresiones faciales, los movimientos, la frecuencia cardíaca o la voz, debido a su fiabilidad limitada, a su falta de especificidad y a su limitada posibilidad de generalizar rasgos. Por tanto, el Reglamento ha prohibido su introducción en el mercado (art. 5.1, d) *quater*), a pesar de que los avances en la materia son notables[104].

Cada vez más, los jueces en USA emplean sistemas de IA para la admisión de la prueba testifical y pericial. Y también para producir pruebas periciales, derivadas del uso, por parte de los peritos, de sistemas de IA de aprendizaje automático, que, a pesar de su apariencia infalible, de veracidad y de objetividad, están sometidos a errores y sesgos, los propios de sus creadores, y a la mala calidad de los datos que usan, hasta el punto en que los jueces son incapaces de saber cómo se ha llegado a los resultados que ofrece el sistema[105].

D. En la Sentencia

A efectos de motivación de la sentencia, la Resolución del Parlamento Europeo de 20 de enero de 2021, sobre Inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho Internacional, en su punto 73 exige que se respete el derecho del funcionario responsable (aquí, el juez o magistrado) a tomar personalmente la decisión y a desviarse de la información recibida de la IA cuando lo considere necesario a la luz de los detalles del asunto en cuestión[106]. Los requisitos que la LEC establece para las Sentencias podrían ser aplicables por analogía a los casos del orden jurisdiccional contencioso-administrativo, como establece la Disposición Final 1ª de la LJCA, que remite a la

102. Nieva Fenoll se muestra partidario de emplear sistemas de IA para validar la coherencia de pruebas testificales pues cree que, en contra de la creencia popular, el juez no debe basarse en la inmediación de lo que ve cuando declara un testigo, pues sus impresiones, lejos de ayudarle a saber si lo que está viendo y oyendo tiene visos de ser cierto, pueden engañarle. Y los sistemas de IA pueden ayudar a rastrear contradicciones en declaraciones de varios testigos. E incluso dentro de la declaración del mismo testigo. Podríamos decir lo mismo de las pruebas documentales, sobre todo de la privada. Y en el caso de las pruebas periciales, sostiene que las herramientas de IA pueden ayudar a los jueces a validar aquellos elementos técnicos que el juez no domina, sobre la base de los criterios *Daubert* (que son una serie de puntos que el juez norteamericano *Blackmun* expuso en la Sentencia del TS que lleva su nombre, confirmados por otras sentencias posteriores del tribunal Supremo de los EE.UU., y recogidos en el art. 702 de las *Federal Rules of Evidence* de 2011): que la técnica usada emplee el método científico; que haya sido objeto de revisión por pares; que indique el grado de error de la técnica empleada; que indique si existen estándares y controles sobre la fiabilidad de la técnica; y que exista consenso de la comunidad científica sobre la técnica empleada. Cfr. Nieva Fenoll 2022a, pp. 95-96.

103. El programa ADVOKATE, fue diseñado para evaluar a los testigos en Glasgow y Edimburgo. El testigo debe responder a una serie de cuestiones. Y eso que no emplea análisis del lenguaje corporal y gestual, ni polígrafos, que serían altamente peligrosos en sede judicial.

104. Cfr. Muñoz Ruiz 2023, pp. 114-115, describe dos de estos sistemas: las gafas detectoras de emociones de la empresa *Humanyze*, que describen las emociones de la persona que es mirada a través de estas gafas, que usan 24 puntos faciales de control, pero que sólo tiene una fiabilidad del 64%. Y el sistema *Converus EyeDetect*, que usa 60 puntos de control de los ojos, y que aspira a sustituir al detector de mentiras al verificar la reacción involuntaria de los ojos (las pupilas y su reacción a la mentira).

105. Cfr. Pereira-Carvalho 2022, pp. 719-720.

106. También se requiere que se mantenga informado al público sobre el uso de la IA en el ámbito de la justicia, y que los usos de la IA no den lugar a discriminación derivada de sesgos de programación; y recalca el derecho de la persona demandada a recurrir la decisión de conformidad con la legislación nacional, sin que se elimine en ningún caso la responsabilidad final del poder judicial.

LEC en lo no previsto por esta Ley. Vienen recogidos en los arts. 216 y 218 de la LEC, y exigen, evidentemente, la intervención humana del juez (garantía de reserva humana o principio de inclusión), que no podría ser sustituido por completo por un sistema de IA experto.

Esos requisitos son:

- Los tribunales decidirán los asuntos en virtud de las aportaciones de hechos, pruebas y pretensiones de las partes, excepto cuando la ley disponga otra cosa en casos especiales.
- Las sentencias deben ser claras, precisas y congruentes con las demandas y con las demás pretensiones de las partes, deducidas oportunamente en el pleito.
- Harán las declaraciones que aquéllas exijan, condenando o absolviendo al demandado y decidiendo todos los puntos litigiosos que hayan sido objeto del debate.
- El tribunal, sin apartarse de la causa de pedir acudiendo a fundamentos de hecho o de derecho distintos de los que las partes hayan querido hacer valer, resolverá conforme a las normas aplicables al caso, aunque no hayan sido acertadamente citadas o alegadas por los litigantes.
- Las sentencias se motivarán expresando los razonamientos fácticos y jurídicos que conducen a la apreciación y valoración de las pruebas, así como a la aplicación e interpretación del derecho. La motivación deberá incidir en los distintos elementos fácticos y jurídicos del pleito, considerados individualmente y en conjunto, ajustándose siempre a las reglas de la lógica y de la razón[107].
- Cuando los puntos objeto del litigio hayan sido varios, el tribunal hará con la debida separación el pronunciamiento correspondiente a cada uno de ellos.

A nivel administrativo el peso del precedente obliga al órgano administrativo a motivar las razones por las que se aparta de él (art. 35.1, c LPAC). A nivel judicial siempre existe una jurisprudencia más o menos consolidada sobre determinados asuntos, fruto de la repetición de casos similares a lo largo de los años, del decantamiento del razonamiento jurídico de los órganos judiciales colegiados (Tribunales). Los jueces y tribunales no tienen obligación de motivar, sin embargo, por qué no se adhieren a una línea jurisprudencial pacífica o principal, acogiéndose a otras o a una propia. Pero imaginemos que los sistemas de IA generativa o de *deep learning* a nivel judicial le ofrecieran al juez, constantemente, una propuesta de resolución judicial de la línea principal o mayoritaria: ¿no se sentiría ese juez o magistrado compelido o presionado a acogerse a ella, o a tener que motivar por qué no lo hace, con la subsiguiente disminución de su libertad de juicio? Me temo que ese tipo de presión se va a dar, y que muchos jueces cederán a ella para que no se produzcan reclamaciones de responsabilidad por parte de los administrados[108]. Este peligro sería tanto mayor cuanto más bajo es el nivel del Tribunal, por razones obvias. Pero es que, además, se puede dar el caso de que se uniformicen las resoluciones judiciales conforme a lo ofertado por la IA, contradiciendo en ocasiones la jurisprudencia de los Tribunales superiores.

En otras ocasiones, se han realizado estudios un poco más profundos, en el orden contencioso-administrativo, con herramientas de IA predictivas, con la intención de unificar la jurisprudencia en asuntos donde había mucha variación en el sentido de las resoluciones, en aras del principio de igualdad, que han dado resultados erráticos, lo que demuestra que estos sistemas están aún en pañales[109]. Sí podrían usarse a la hora de, por ejemplo,

107. Ello no quita para que en determinados casos donde la jurisprudencia es pacífica, las herramientas de IA pueda ofrecer "motivaciones tipo" que puedan ser fácilmente adaptables a cada caso similar que se produzca, intercambiables para casos semejantes.

108. Es la misma presión que tendrá un cirujano o un médico al que la IA le indique que tal tejido es canceroso, aunque él no lo tenga tan claro. O al contrario. ¿Tendrá ese médico o cirujano la personalidad, la autoridad y el valor suficientes como para apartarse de un diagnóstico médico realizado por IA tras analizar todos los datos del paciente en forma de radiografías o resonancias magnéticas?

109. Caso de la herramienta de IA JURICA: por iniciativa del Ministerio de Justicia de Francia se compararon los resultados en el contencioso de los tribunales de apelación de Rennes y de Douai, en la primavera de 2017. Los resultados fueron fallidos, pues la máquina no lograba distinguir cuestiones lexicales de los verdaderos razonamientos usados para resolver un caso. Vid. Ronsin 2017.

en el contencioso, establecer determinadas horquillas de indemnización razonables (derivadas del manejo de datos previos de las circunstancias del caso, de los daños producidos, de la intencionalidad, del estándar de servicio, etc.) en casos de responsabilidad patrimonial (baremos por accidente de tráfico, por ejemplo, y otros), de infracciones administrativas, del coste de reparación de la situación al estado inicial, de indemnización de despido de personal público, de valoración de méritos en oposiciones, concursos o acreditaciones, y otras cuestiones materiales.

La motivación de la sentencia reclama transparencia de los algoritmos y de los sistemas de IA empleados. La propuesta de Reglamento IA de la UE exige que los usuarios tengan derecho a comprender cómo funcionan, su finalidad, y la forma de uso, mediante instrucciones que se incorporen al software por parte de su proveedor (art. 13 de la propuesta de Reglamento). El Parlamento europeo introdujo en junio de 2023 un apartado iii *bis* del art. 13.3, b), que rechaza el empleo de cajas negras: se deberá dar información… *del grado en que el sistema de IA pueda ofrecer una explicación de las decisiones que adopte*. Y en su Anexo IV exige que las instrucciones técnicas del sistema faciliten información sobre cómo funcionan sus algoritmos, lo que supone, una vez más, una restricción de las cajas negras (véase apdos. 2°, b, f y 3°).

La reserva de humanidad o supervisión humana (aquí, los jueces) es esencial en la sentencia. Y procede, sin duda, del art. 47 de la Carta de Derechos fundamentales de la UE[110]. Pero aparece también recogida en la propuesta de Reglamento. En concreto en su art. 14, que indica que los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cosas[111]. No es posible, por tanto, y estaría prohibido en la regulación europea que las resoluciones judiciales las den las máquinas, sin control humano (robotización judicial). En el apdo. 4° de este precepto se advierte a los usuarios de estos sistemas (aquí serían los jueces) a que sean conscientes de la tentación de confiar automáticamente o en exceso en la información de salida generada por un sistema de IA de alto riesgo ("sesgo de automatización"), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión (sentencias u otras resoluciones judiciales). Y esos jueces deben estar debidamente formados para usar estos sistemas (art. 29.1 *bis*, ii de la propuesta de Reglamento).

E. Legaltech

Es inevitable que las herramientas de *Legaltech* de los bufetes y otras empresas acostumbradas a los pleitos usen herramientas de predictibilidad con los nombres de los jueces y de los abogados, los casos ganados o vencidos y el sentido de la resolución[112]. Por ejemplo, Tirant lo Blanch y WoltersKluwer están desarrollando herramientas de

110. «Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley».

111. Se ha añadido como Enmienda en el Parlamento que las personas físicas encargadas de garantizar la vigilancia humana tendrán un nivel suficiente de alfabetización en materia de IA de conformidad con el artículo 4 *ter* y contarán con el apoyo y la autoridad necesarios para ejercer esa función durante el período en que los sistemas de IA estén en uso y para permitir una investigación exhaustiva tras un incidente.

112. Estas herramientas de IA predictivas a primera vista no alteran en nada los resultados de la actuación de los profesionales que actúan a diario en la justicia, salvo el hecho de que el juez podría inhibirse de asuntos sensibles o políticamente incorrectos, por miedo de que su nombre se asocie a casos, por ejemplo, de condenas a mujeres por denuncias falsas por violencia de género a hombres, o a casos de lesiones graves de salud derivadas del empleo de las terapias genéticas impuestas a la población con ocasión del Covid, o de casos en que el desarrollo económico deba prevalecer sobre la protección ambiental, etc., por poner tres ejemplos actuales reprobados por el pensamiento único. A nivel de tribunales (órganos judiciales colegiados) sería importante, desde luego, incluir información sobre los jueces discrepantes del voto mayoritario. También puede ocurrir que se produzca una desigualdad entre los abogados autónomos que trabajen sin IA de los que trabajen en grandes bufetes, que sí pueden permitirse el empleo de instrumentos de IA, y ofrecerles a sus clientes cierta seguridad a la hora de pleitear o no. Los Colegios oficiales deberían ofrecer esta herramienta, al menos en su versión beta, para todos los colegiados.

jurimetría (o justicia predictiva), que son programas o *software* que permiten al abogado preparar mejor su estrategia procesal, en la medida en que los sistemas de IA organizan megadatos relacionados con el caso (línea jurisprudencial a seguir más segura para ganarlo), el juez (cómo sentencia según qué casos, cuál es mejor para nuestro asunto), el tribunal que sentencia (tiempo de espera, colapso de distintas salas o secciones, etc.), la parte pública y privada a la que se enfrenta (veces que gana o pierde, sus líneas de defensa, todo ello según el caso), abogados (porcentaje de casos ganados y según los tipos de caso del abogado al que se enfrenta, su preparación, etc.).

Esta práctica, en Francia, está prohibida por usar los nombres de los jueces[113], y porque afecta a su independencia[114], por medio del art. 33 de la Ley 2019-222, de 23 de marzo, de programación 2018-2022 y reforma para la justicia, que impuso penas de hasta 5 años de cárcel a quienes reutilicen los datos personales de los jueces con el fin de analizar, evaluar, comparar o predecir sus prácticas judiciales, o los perfiles de rendimiento de los abogados. De hecho, han sido los jueces franceses y el Consejo General de la Abogacía francés los que han estado detrás de esa prohibición.

Uno se pregunta si, a este paso, la profesión de abogado acabará siendo reemplazada por la jurimetría, pues el estudio de la viabilidad del caso ya lo puede hacer el software correspondiente; y el trabajo de argumentación jurídica de la demanda, de las medidas cautelares, de la práctica de las pruebas o de las conclusiones, cada vez más, puede acabar siendo realizado también por estos sistemas.

En opinión de Suárez Xavier, las empresas que venden estos sistemas de Legaltech o *Lawtech* deberían inscribirse en el Colegio profesional de abogados y procuradores, pues deben ser calificadas de sociedades profesionales, conforme al art. 1 de la Ley 2/2007, de 15 de marzo, de Sociedades profesionales[115]. El Consejo General de la Abogacía Española debería establecer unos principios y garantías para su uso, con respeto a las competencias de los Consejos autonómicos y a los Colegios.

Publicitar los nombres de los jueces en las sentencias y resoluciones judiciales es obligatorio, conforme al principio de juicio público del art. 6 CEDH, pero no así de los abogados privados, de los abogados del Estado o letrados de las Comunidades Autónomas o de las entidades locales. Recordemos que la normativa de protección de datos personales en el proceso se encuentra en los arts. 236 *bis* a *decies* de la LOPJ, y que se rige por el principio de proporcionalidad y de consentimiento. Sí ocurre así en los Estados Unidos, donde estas herramientas de IA realizan rankings de abogados conforme a sus casos ganados o perdidos, o el historial de litigios de jueces, abogados y bufetes

113. En Francia, desde 2019, se ha prohibido la jurimetría que implica a los jueces, vetando el tratamiento y divulgación de los datos de los procesos judiciales, conforme al art. 33 de la Ley nº. 222/2019: «los datos de identidad de los magistrados y miembros del registro no pueden ser reutilizados con el propósito o efecto de evaluar, analizar, comparar o predecir sus prácticas profesionales reales o presuntas». Y se imponen sanciones a los que incumplan esta prohibición. No se prohíben las herramientas de legaltech, pero se prohíbe que se elaboren perfiles de los jueces o magistrados. En España no se ha producido tal prohibición, a pesar de que el CGPJ podría haberlo hecho, pues tiene atribuida desde 2019 la competencia, por el art. 560.1, 16ª, e) de la LOPJ, para ejercitar la potestad reglamentaria en materia de publicación y reutilización de sentencias judiciales. Esa atribución la realizó la Ley Orgánica 4/2018, de 28 de diciembre, de reforma de la LOPJ. Pero es imposible que por la vía reglamentaria se puedan regular aspectos de IA, que puede afectar a los derechos fundamentales, sin el necesario rango de ley orgánica. Actualmente carecemos de marco legal, ya que el Reglamento 3/2010, del CGPJ, sobre reutilización de sentencias y otras resoluciones judiciales fue anulado por la STS (Sala 3ª), de 28 de octubre de 2011, Ponente Conde Martín de Hijas, por falta de competencia del CGPJ para reglamentar la actividad de reutilización de sentencias, al entender que se trata de una actividad que realizan terceros ajenos al poder judicial (la empresa Aranzadi, entre ellos), y por tanto no se sitúa dentro del ciclo institucional de los órganos del Poder Judicial, en concreto dentro de la actuación del Consejo en materia de publicación oficial o difusión de la jurisprudencia.

114. Cfr. Suárez Xavier 2023, p. 115, considera igualmente que el perfilado o jurimetría (o justicia predictiva) de los jueces puede acabar afectando a la independencia judicial.

115. Cfr. Suárez Xavier 2023, pp. 143-144.

de abogados, incluidas las tasas de éxito para juicios en comparación con los competidores, tasas de éxito de diferentes tipos de demanda y según demandante y demandado[116]. No nos parece que este tipo de perfiles, salvo el de los jueces, sea contraproducente, pues se realizan en realidad en muchas profesiones privadas y públicas.

F. ¿Juez robot?

¿Sería posible llevar a cabo juicios electrónicos (ODR, *online dispute resolution*) en determinados procedimientos sencillos en el orden jurisdiccional contencioso-administrativo? Sí sería posible, por ejemplo, en casos tributarios de escasa importancia a nivel local, donde las potestades son regladas (y su correspondiente juicio posterior ante los Juzgados de lo contencioso-administrativo) pero en los casos en que se pone en tela de juicio el resultado de una potestad discrecional tal cosa sería desaconsejable e imposible. Ello porque este tipo de *chatbots* se limitan a extraer una conclusión de una serie de premisas que establecen haciendo preguntas a ambas partes, preguntas que se derivan de los requisitos reglados que exige la legislación en cuestiones de sencilla solución, en los que sólo cabe A o B. Como quiera que la mayoría de los litigios en el contencioso derivan de potestades discrecionales (sancionadora, expropiatoria, discrecionalidad técnica en asuntos de empleo público, de planeamiento o de ejecución urbanística, de planeamiento ambiental, inspectora y revisora, etc.). Incluso en cuestiones de ejecución forzosa hay cierta discrecionalidad en la elección del medio de ejecución y de su cuantificación. En materia tributaria local o en materia de licencias regladas, incluso de servicios públicos o de subvenciones (cuando sean reglados) tal cosa podría ser posible. Habría que investigarlo y probarlo. Y siempre que el administrado acepte voluntariamente este tipo de ODR y que pueda acceder posteriormente a un recurso de apelación[117].

También debería ser posible que este tipo de ODR fuera fácilmente accesible al gran público, sin que existieran barreras informáticas de difícil solución. Incluso el empleo de procesamiento de lenguaje oral debería ser exigible.

La posibilidad de acceso a herramientas de IA por parte de los letrados de la Administración demandada (que suelen ser muy caras y de difícil manejo y a las que esa Administración podría estar suscrita) en el contencioso-administrativo y no por la parte de la parte privada o demandante (que puede tener un letrado más modesto y sin acceso a esos sistemas) puede provocar una afectación al principio de igualdad procesal. También al principio de audiencia o contradicción, si la parte privada no puede tener acceso al algoritmo que emplee el Juez o la Administración demandada durante el proceso.

8. Conclusión

El riesgo de la fascinación de la máquina, del Golem, de la recreación del mundo desde lo humano imperfecto a la máquina perfecta, revolotea desde hace años sobre el mundo jurídico. Y, más recientemente, en el ámbito judicial.

En esta investigación hemos abogado por el empleo de de sistemas de IA débiles, es decir, aquéllas no generativas, y, especialmente, en el contencioso-administrativo: los que sirven de apoyo a la labor del juez, con un mejor tratamiento y uso de los datos de jurisprudencia, doctrina legal y doctrina académica, aunque incluso en estos casos la labor del juez es imprescindible, para motivar sus resoluciones, como exige el art. 218 de la LEC. También son loables las herramientas o sistemas de IA que sirven para gestionar o impulsar los procesos, como LEXNET, el expediente electrónico y la automatización de datos. Rechazamos el empleo de sistemas de IA generativa, por la inquietante amenaza que producen contra los derechos fundamentales de los administrados. Por supuesto, un juez-persona nunca podrá en España ser reemplazado por un juez-robot, debido al principio de exclusividad del art.117.3 CE y al derecho al juez predeterminado por ley del derecho a la tutela judicial efectiva del art. 24 CE.

A pesar de esta premisa, hemos indagado sobre la posibilidad del uso de sistemas de IA en algunos trámites del contencioso-administrativo, con las limitaciones éticas y jurídicas que impone el

116. Por ejemplo, Premonition, con sede en Nueva York. Cfr. Roberto Granero 2022, p. 111.

117. Vid. la Resolución 2054 (2015) de la Asamblea Parlamentaria del Consejo de Europa, de 10 de noviembre, "Equality and non-discrimination in the access to justice".

Derecho internacional, hasta ahora *soft law* y propuestas de regulación, como el Reglamento de IA de la UE y el Convenio Marco del Consejo de Europa.

El sueño de las máquinas podría convertirse en una pesadilla digital. Nuestro Estado de Derecho podría degenerar en una especie de "Estado algorítmico de Derecho", expresión acuñada por Barrio Andrés[118] en un sentido positivo, pero que, en mi opinión, encierra una contradicción interna irresoluble, ya que no hay nada más dictatorial que un algoritmo, por ser inexorable, mecanicista y separado de toda lógica de compasión o caridad humana, y también de prudencia jurídica. Una especie de Estado policía total, con internet de las cosas, datos subidos en tiempo real a la nube, decisiones tomadas por máquinas mediante *big data*, publicad institucional mediante *blockchain* juicios resueltos por IA sin participación humana, servicios públicos prestados de forma virtual, etc. conformarían una distopía que podría no estar muy lejana, y que ni siquiera Orwell podría haber soñado.

Bibliografía

A. Abadías Selma (2022), *Justicia juvenil e inteligencia artificial en la era de la cultura "Touch"*, Tirant lo Blanch, 2022

J.D. Ayllón García (2020), *La inteligencia artificial como un medio para administrar justicia*, in F. Bueno de Mata (dir.), I. González Pulido (coord.), "Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia", Comares, 2020

S. Barona Vilar (2022), *La digitalización y la algoritmización, claves del nuevo paradigma de justicia eficiente y sostenible*, in I. Colomer Hernández (dir.), M.Á. Catalina Bevanente, S. Oubiña Barbolla (coords.), "Uso de la información y de los datos personales en los procesos: los cambios en la era digital", Aranzadi-Thomson-Reuters, 2022

S. Barona Vilar (2021), *Algoritmización del derecho y la justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, 2021

M. Barrio Andrés (2023), *Chatgpt y su impacto en las profesiones jurídicas*, in "Diario La Ley", n° 10289, 2023

M. Barrio Andrés (2020), *Manual de Derecho digital*, Tirant lo Blanch, 2020

M. Barrio Andrés (2020a), *Retos y desafíos del Estado algorítmico de Derecho*, ARI 82/2020, Real Instituto Elcano, 9 de junio de 2020

A.D. Berning-Prieto (2023), *La naturaleza jurídica de los algoritmos*, in E. Gamero Casado (dir.), F.L. Pérez Guerrero (coord.), "Inteligencia artificial y sector público: retos, límites y medios", Tirant lo Blanch, 2023

J.R. Chaves García (2018), *En puertas del procedimiento abreviado electrónico*, in "delaJusticia.com", 2018

Consejo de Europa (2018), *Carta Ética Europea sobre el uso de inteligencia artificial en los sistemas judiciales*, 2018, n. 126

M. De Hoyos Sancho (2021), *El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea*, in "Revista General de Derecho Procesal", 2021, n. 55

A. De Miguel Asensio (2023), *Manual de Derecho de las Nuevas Tecnologías*, Aranzadi, 2023

J.A. Eguíluz Castañeira (2020), *Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales*, in "Estudios de Deusto", vol. 68, 2020, n. 2

118. Vid. Barrio Andrés 2020a.

E. Gamero Casado (2023), *Las garantías de régimen jurídico del sector público y del procedimiento administrativo común frente a la actividad automatizada y la inteligencia artificial*, in E. Gamero Casado, F.L. Pérez Guerrero (coords.), "Inteligencia artificial y sector público: retos, límites y medios", Tirant lo Blanch, 2023

I. Gaudemet (2018), *La justice à l'heure des algorithmes*, in "Revue du Droit publique", 2018, n. 3

E.M. Gil Cruz (2021), *Función instrumental de la inteligencia artificial en la determinación de los conceptos jurídicos indeterminados*, in "Revista Aranzadi Doctrinal", 2021, n. 8

Y.N. Harari (2017), *Homo Deus: A Brief History of Tomorrow*, Penguin Random House, 2017

F. Martín Diz (2019), *Inteligencia artificial y proceso: Garantías frente a eficiencia en el entorno de los derechos procesales fundamentales*, in F. Jiménez Conde (dir.), R. Bellido Penadés (dir.), P. Llopis Nadal, Elena de Luis García (coords.), "Justicia: ¿garantías "versus" eficiencia?", Tirant lo Blanch, 2019

R. Martínez Gutiérrez (2019), *Los retos de la innovación tecnológica en la jurisdicción contencioso-administrativa*, in F. López Ramón, J. Valero Torrijos (coords.), "20 años de la Ley de lo Contencioso-administrativo", Actas del XIV Congreso de la AEPDA, INAP, 2019

R. Martínez (2017), *Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos*, in "Dilemata", 2017, n. 24

V.M. Moreno Catena (2022), *Los datos en el sistema de justicia y la propuesta de Reglamento UE sobre inteligencia artificial*, in M.A. Catalina Benavente, S. Oubiña Barbolla (coords.), Ignacio Colomer Hernández (dir.), "Uso de la información y de los datos personales en los procesos: los cambios en la era digital", Thomson Reuters Aranzadi, 2022

A.B. Muñoz Ruiz (2023), *Biometría y sistemas automatizados de reconocimiento de emociones. Implicaciones jurídico-laborales*, in "Labos", vol. 4, 2023, n. 2

P.L. Murillo de la Cueva (2003), *La Constitución y el derecho a la autodeterminación informativa*, in "Cuadernos de Derecho Público", 2003, n. 19-20

Y. Murillo Paños (2021), *Casos de uso de Inteligencia Artificial aplicados a herramientas de informática judicial,* in F. Bueno de Mata (dir.), I. González Pulido (coord.), "Fodertics 9.0. Estudios sobre tecnologías disruptivas y justicia", Comares, 2021

J. Nieva Fenoll (2022), *Inteligencia Artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino*, in "Revista General de Derecho Procesal", 2022, n. 57

J. Nieva Fenoll (2022a), *Un cambio generacional en el proceso judicial: la inteligencia artificial*, in C. Villegas Delgado, P. Martín-Ríos (eds.), "El derecho en la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial", Tirant lo Blanch, 2022

C. O'Neil (2017), *Armas de Destrucción Matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, 2017

M. Olmedo Palacios (2023), *Legal tech y Administración de justicia en España*, in M. Barrio Andrés (dir.), "Legal Tech. La transformación digital de la abogacía", La Ley, 2023

A. Ortega (2021), *Hacia un régimen europeo de control de la Inteligencia Artificial*, ARI 52/2021, Real Instituto Elcano, 6 de mayo de 2021

S. Ortiz Hernández, I. Garrós Font, N. Romera Santiago (2020), *Hacia la implantación de la inteligencia artificial en nuestro sistema judicial*, in "Revista Aranzadi Doctrinal", 2020, n. 3

D. Palomo Vélez, D. Valdés Quinteros (2023), *Inteligencia artificial y factor humano de cara a las garantías judiciales. En especial de la motivación de las sentencias*, in D. Vallespín Pérez (dir.), J.M. Asencio Gallego (coord.), "Inteligencia artificial y proceso. Eficiencia vs. Garantías", Juruá Editorial, 2023

V. Pérez Daudí (2022), *De la justicia a la ciberjusticia*, Atelier, 2022

V. Pérez Daudí (2022a), *La previsibilidad judicial y la aplicación de la inteligencia artificial a la adopción de las resoluciones judiciales*, in I. Colomer Hernández (dir.), M.Á. Catalina Bevanente, S. Oubiña Barbolla (coords.), "Uso de la información y de los datos personales en los procesos: los cambios en la era digital", Aranzadi-Thomson-Reuters, 2022

M.J. Pérez Estrada (2022), *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Tirant lo Blanch, 2022

J. Ponce Solé (2019), *Inteligencia artificial, Derecho Administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*, in "Revista General de Derecho Administrativo", 2019, n. 50

H. Roberto Granero (2022), *Derechos y garantías concretas frente al uso de inteligencia artificial y decisiones automatizadas, especialmente en el ámbito judicial y de aplicación de la ley*, in L. Cotino Hueso (dir.), M. Bauzá Reilly (coord.), "Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas", Aranzadi, 2022

L.R. Rodríguez Oconitrillo, J.J. Vargas, Á. Burgos, J.M. Corchado (2021), *Representación del conocimiento: novedoso método para procesar la interpretación y valoración de los hechos y pruebas que hace un juez en el análisis de casos jurídicos*, in F. Bueno de Mata (dir.), I. González Pulido (coord.), "Fodertics 9.0. Estudios sobre tecnologías disruptivas y justicia", Comares, 2021

X. Ronsin (2017), *L'utilisation de l'outil Predictice déçoit la cour d'appel de Rennes*, in "Dalloz Actualité", 16 octobre 2017

I. Salazar García (2022), *Retos actuales de la ética en la inteligencia artificial*, in L. Cotino Hueso (dir.), M. Bauzá Reilly (coord.), "Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas", Aranzadi, 2022

A. Salom Lucas (2021), *Inteligencia artificial y proceso*, in "Revista Aranzadi de Derecho y Nuevas Tecnologías", 2021, n. 57

F. Silva Pereira, A.S. De Magalhaes e Carvalho (2022), *Inteligencia artificial como medio de prueba en procesos civiles*, in F. Bueno de Mata (dir.), I. González Pulido (coord.), "Fodertics 10.0. Estudios sobre derecho digital", Comares, 2022

A. Simoncini, E. Longo (2021), *Fundamental Rights and the Rule of Law in the Algorithmic Society*, in H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), "Constitutional Challenges in the Algorithmic Society", Cambridge University Press, 2021

P.R. Suárez Xavier (2023), *Justicia Predictiva: construyendo la justicia del Siglo XXI*, Aranzadi, 2023

S. Tierno Barrios (2020), *La Administración de Justicia bajo el prisma de la inteligencia artificial*, F. Bueno de Mata (dir.), I. González Pulido (coord.), "Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia", Comares, 2020

D. Vallespín Pérez (2023), *Prólogo*, in J.D. Vallespín Pérez (dir.), J.M. Asencio Gallego (coord.), "Inteligencia artificial y proceso. Eficiencia vs. Garantías", Juruá Editorial, 2023

D. Vallespín Pérez (2023a), *"Robotización" de la valoración de la prueba en el proceso civil español*, in D. Vallespín Pérez (dir.), J.M. Asencio Gallego (coord.), "Inteligencia artificial y proceso. Eficiencia vs. Garantías", Juruá Editorial, 2023

C. Villegas Delgado (2023), *Gobernanza algorítmica, ética de las inteligencia artificial y estado (algorítimico) de derecho: retos para el jurista en la era digital*, in D. Vallespín Pérez (dir.), J.M. Asencio Gallego (coord.), "Inteligencia artificial y proceso. Eficiencia vs. Garantías", Juruá Editorial, 2023

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0119 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Filippo Bagni

The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act

The article carries out an analysis of the innovative tool known as "regulatory sandbox", investigating its specific features in both abstract and concrete terms through the investigation of relevant European use cases. Through the analysis of the application of the regulatory sandbox in the specific field of the regulation of artificial intelligence, with particular reference to the discipline envisaged by the European regulation proposal called "Artificial Intelligence Act", the article aims at verifying the possible applications and implications of this instrument also in the field of cybersecurity, with a specific focus on the recent European regulation proposal still under negotiation called "Cyber Resilience Act".

Regulatory sandbox – Artificial intelligence – Artificial Intelligence Act – Cybersecurity – Cyber Resilience Act

La sandbox regolamentare e la sfida a tema cybersecurity: dall'Artificial Intelligence Act al Cyber Resilience Act

L'articolo analizza lo strumento innovativo denominato "sandbox regolamentare", indagandone le caratteristiche in termini astratti e concreti attraverso l'analisi di rilevanti casi di studio a livello europeo. Operando uno studio attento dell'applicazione dello strumento della sandbox regolamentare nell'ambito della regolamentazione dell'intelligenza artificiale, con particolare riferimento alla proposta di regolamento europeo denominata "Artificial Intelligence Act", l'articolo si propone di verificare le possibili applicazioni e implicazioni di questo strumento anche nel campo della cybersecurity, con un focus specifico sulla recente proposta di regolamento europeo ancora in fase di negoziazione denominata "Cyber Resilience Act".

Sandbox regolamentare – Intelligenza artificiale – Artificial Intelligence Act – Cybersecurity – Cyber Resilience Act

The Author is PhD student in Cybersecurity at IMT School for Advanced Studies, Lucca, Italy

1. Introduction

The article aims to conduct an analysis of the regulatory sandbox instrument and its potential application concerning cybersecurity, with specific reference to the recent European proposal known as the "Cyber Resilience Act"[1].

The purpose of the paper is primarily to investigate the regulatory sandbox as an innovative and next-generation regulatory tool, exploring its peculiarities and key characteristics to better understand its true potential. In doing so, the inquiry will not be abstract but rather focus on analysing existing use cases, aiming to define its objectives and actual operational dynamics.

Moreover, the investigation will emphasize the increasing importance of the regulatory sandbox as a privileged hybrid instrument for regulating new technologies, particularly in the digital domain. Hence, the aim is to highlight its increasingly European dimension by examining its latest experimental applications in the crucial and controversial field of artificial intelligence regulation.

Lastly, the final endeavour is to explore the possible applications of the regulatory sandbox in the context of cybersecurity. This complex theme is gaining growing importance at the European level, and yet it seems not to have explicitly embraced the use of the regulatory sandbox so far. The article will try to understand the reasons why.

The entire scientific inquiry, as previously mentioned, will have the advantage of examining the regulatory sandbox tool from a practical and concrete perspective, analysing existing use cases, future European projects, and the provisions set forth by some of the most significant ongoing European regulations in the field of technology regulation (the "Artificial Intelligence Act" proposal and the "Cyber Resilience Act" proposal).

In particular, the paper is structured into four parts: (a) the initial segment entails an examination of the regulatory sandbox instrument in a broader context, thoroughly exploring its fundamental characteristics and operational aspects; (b) the subsequent section is dedicated to scrutinizing pertinent use cases of sandboxes at a national level across various sectors (finance, privacy, and digital technology); (c) the third segment provides a comprehensive analysis of the structuring of the European sandbox instrument at the European level, focusing on the regulatory framework proposed in the Artificial Intelligence Act proposal and the Spanish pilot sandbox initiative on artificial intelligence; (d) lastly, the fourth and concluding part is dedicated to examining the Cyber Resilience Act proposal and the potential applications of the sandbox instrument within the cybersecurity domain.

2. The "Regulatory Sandbox": definition, characteristics, and operational scope

The challenges posed by technological transformation and the emergence of new products and

1. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454.

services have brought about new regulatory complexities[2]. The flexibility of technological progress has tested the capabilities of lawmakers and their inherent regulatory rigidity[3]. Consequently, new regulatory approaches have been developed (some even termed "experimental lawmaking")[4], including the incorporation of "experimentation clauses"[5]. These legal provisions grant enforcing authorities a certain degree of flexibility in dealing with innovative technologies, products, or approaches, even if they do not fully comply with existing legal requirements[6].

These clauses lay the groundwork for novel legal experimentation. It is in light of these provisions that the concept of true regulatory experimentation spaces, known as "regulatory sandboxes"[7], has emerged and gained momentum. A uniform and standardized definition of the regulatory sandbox is not yet established. The term "sandbox" invokes two parallel images – on one hand, the world of playgrounds where children can play safely and freely, and on the other hand, the realm of computing, where it describes an isolated testing environment that allows system monitoring and prevents harmful programs from damaging the computer system[8]. The addition of the term "regulatory" refers to a tool designed to test new services and products in an artificially created regulatory environment.

A regulatory sandbox can be described as a model that allows companies to test innovations within a controlled real-world environment under a specific framework developed and monitored by a competent authority[9]. There is no one-size-fits-all sandbox model, as it may vary case by case based on the type of technology, the sector of experimentation, the overseeing authority, and other factors.

A regulatory sandbox refers to a controlled experimentation space where entities operating in regulated sectors (e.g., banking, finance, and insurance) or highly technological areas (e.g., artificial intelligence systems, digital products) can test their innovative products and services for a limited period[10]. During this designated time, the experimentation occurs in constant dialogue with supervisory authorities responsible for verifying the compliance of the innovative product/service before market entry, potentially benefitting from a simplified transitional regime. The true added value of the regulatory sandbox lies in the opportunity to "make mistakes" and experiment with a product that is not yet compliant with the existing regulations, under the close guidance of regulators. The

2. A deep analysis of the complex tension between the economic and social benefits of innovation and the risks associated with, is available at Weimer-Marin 2016, pp. 469-474.
3. For an in deep analysis of the difficulties related to regulate innovation see Bennett Moses 2013.
4. Cf. Ranchordas 2021. For a more detailed analysis of the innovative side of the regulation tool see also Ranchordas 2015.
5. For a detailed analysis of the experimental method see: van Gestel-van Dick 2011; Mousmouti 2018; Heldeweg 2015.
6. Cf. European Commission 2023, p. 178 ss. For more on this point see also Attrey-Lesher-Lomax 2020. For a doctrinal analysis of the Better regulation see Radaelli, 2007; Wiener 2006; Baldwin 2005.
7. Cf. European Commission 2023, p. 131: «Technological transformation, the emergence of new products, services, and business models can be quite challenging from a regulatory perspective. To enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority, a relatively new policy instrument – a 'regulatory sandbox' – can be set up».
8. Cf. Yordanova 2019.
9. Cf. European Commission 2023, p. 599 ss.
10. This is the definition of regulatory sandboxes provided by the Council: «Concrete frameworks which, by providing a structured context for experimentation, enable where appropriate in a real-world environment the testing of innovative technologies, products, services or approaches (…) for a limited time and in a limited part of a sector or area under regulatory supervision ensuring that appropriate safeguards are in place». Cf. Council of the European Union, *Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age*, doc. 13026/20, 16 November 2020, p. 4.

ultimate goal is to develop an innovative product/service that aligns with the rules of the European market by the end of the experimentation period.

Sandboxes serve a dual purpose: (a) they foster business learning, development, and experimentation of innovations in a real-world environment, and (b) they support regulatory learning by formulating experimental legal frameworks to guide and support businesses in their innovative activities under the supervision of regulatory authorities.

The underlying logic of the sandbox revolves around a traditional win-win scenario. On one hand, it supports market growth and evolution by not hindering but rather facilitating the introduction of technologically innovative products and services. On the other hand, it ensures adequate consumer protection and competition levels, achieved through close dialogue with the regulatory authority. Furthermore, while the company develops a product within a space providing guidelines and (under certain conditions) allowing special regulatory exemptions, the regulatory body gains insight into the operator's activities, thus acquiring new technical expertise through continuous dialogue.

Despite the variety of sandboxes in today's landscape, some common characteristics can be identified[11]. Firstly, the regulatory sandbox applies to innovative products/services not yet available in the market that provide added value to consumers or society at large (e.g., contributing to policy objectives such as environmental protection). Moreover, the product/service's development level must be sufficiently advanced to allow for immediate experimentation (neither too embryonic nor too advanced to preclude modifications), and the activity to be tested must demonstrate economic sustainability throughout the experimentation period. Finally, to identify the appropriate institutional interlocutor, the applicable legislation, and the legislative obstacle on which the product/service seeks to be tested in terms of compliance must be identified.

For the participating operator, guaranteeing legal predictability is essential. The boundaries and terms of a sandbox must be established ex-ante, preferably by law or through protocols of understanding with market surveillance authorities. It is necessary to define legislation and sectors covered by the test, the regulatory exemptions envisaged, access rules, duration, and exit conditions clearly, to facilitate measurement and evaluation of sandbox results. Additionally, even though it is a controlled environment, adequate safeguards must still be in place (e.g., security during tests on autonomous vehicles).

Practically, participation in the regulatory sandbox is subject to admission, monitoring, and evaluation by the regulatory authority, limited to a specific number of participants. The authority typically opens temporary windows (open calls), inviting interested operators to participate by presenting their projects. Once the window is closed, a selection and interview process follow, leading to the definition of admitted projects and the commencement of the experimentation project.

This structure presents both advantages and disadvantages. On the positive side, companies have the opportunity to test their innovations in a real-world context and gain a better understanding of applicable norms. Participation in a sandbox can also facilitate access to financing and reduce the time-to-market. From the regulator's perspective, sandboxes allow for a certain degree of flexibility without sacrificing regulatory standards, facilitating learning in highly complex sectors that are challenging to regulate.

However, there are also disadvantages to consider. Firstly, regulatory sandboxes may increase the risks of market regulation fragmentation if there is no common approach, leading to different outcomes across the EU. Secondly, these instruments require dedicated resources, time, and expertise from both parties (companies and regulators), which smaller companies may not always be able to afford. Thirdly, participation in a sandbox typically does not automatically guarantee product/service compliance and risk-free market entry. Lastly, from an operational standpoint, sandboxes present multiple complexities (e.g., which and how many stakeholders to involve and for how long; how to select participating companies and how many; which product/service characteristics

11. For a detailed analysis of experimental legislation in the EU, see Ranchordas 2021a.

identify it as innovative and advantageous; what are the sandbox objectives and limitations; how to monitor sandbox development; how to evaluate final results), in addition to specific technical complications related to the individual reference sector (banking, insurance, finance, technology, digital)[12].

All these elements must be clarified from the outset with utmost clarity and transparency to ensure the smooth functioning of the sandbox.

3. Relevant national sandbox use cases

The phenomenon of regulatory sandboxes is rapidly gaining momentum and already boasts numerous experiences at both European and international levels across various sectors[13]. In particular, in recent years the tool has gained significant importance throughout the European Union as a means to assist regulatory authorities in addressing the development and use of emerging technologies, such as artificial intelligence and blockchain technologies, as well as in the fields of transportation (e.g., autonomous vehicles or drones), energy (e.g., smart meters), telecommunications (e.g., 5G deployment), and healthcare (e.g., services and innovations for early predictive disease diagnosis).

The first instances of sandbox experimentation in Europe were observed in the Fintech domain[14], owing to its high technicality and substantial sector-specific regulatory oversight[15]. In this context, it is interesting to analyse the use case developed by the Bank of Italy[16].

This is a regulatory sandbox introduced through explicit legislative provisions[17], to increase opportunities for dialogue between the Bank of Italy and businesses. Notably, the Bank of Italy has adopted a complex experimentation scheme for the Fintech sector based on three pillars: the "Fintech Channel", which consists of an Innovation Hub established in 2017 as regulatory support; the "Milan Hub", introduced in 2020 as a place for research initiatives, specifically focused on the project development phase of innovative products; and finally, the regulatory sandbox, introduced in 2021.

The Bank of Italy's sandbox targets technologically innovative products/services that impact the banking, financial, and insurance sectors. Both European and international operators can apply for experimentation for a maximum period of 18 months (renewable). During the year, specific time windows are provided within which companies can apply for admission to the sandbox through a "Fintech Committee" specifically established at the Italian Ministry of Economy. If the Committee's decision is positive, the experimentation begins, during which the Bank of Italy can grant authorizations and provisional derogations based on a clear and pre-established list[18].

12. For a more detailed analysis see European Commission 2023, p. 600 ss.
13. The World Bank report on regulatory sandboxes identified No. 73 programmes in 57 jurisdictions, with the majority of use cases focused on the FinTech environment, many of them powered by artificial intelligence. The overall conclusion of the reports is that such experimentation has the advantage of providing the empirical evidence needed to validate the decisions of regulators. It also assists them in introducing regulatory changes and influencing the design of new supervisory methodologies. For companies, the sandbox survey has resulted in a faster route to market and a better understanding of the regulatory hurdles they must overcome. Cf. World Bank Group 2020.
14. For a deeper insight into the limits and opportunities of sandboxes in the Fintech domain see: Omarova 2020; Allen 2019; Attrey-Lesher-Lomax 2020; Buckley-Arner-Veidt-Zetzsche 2020; Bromberg-Godwin-Ramsay 2017.
15. For a more detailed analysis see: European Banking Authority 2019; European Parliament 2020; Hellmann-Montag-Vulkan 2022.
16. The Bank of Italy is the central bank of the Republic of Italy. It is a public-law institution regulated by national and European legislation. More information available at Bank of Italy official webpage.
17. The sandbox at the Bank of Italy was introduced in implementation of the "FinTech Committee and Experimentation Discipline" laid down in Ministry of Economy and Finance Decree No. 100 of 30 April 2021.
18. In particular, there are four main requirements for admission to the experimentation phase: (1) the activity must utilize innovative technologies that contribute to offering genuinely new and different services/products in the banking, financial, and insurance sectors (the elements of novelty in the project must be demonstrated); (2) the activity must bring added value, alternatively, for end-users (e.g., improved customer experience), for the ef-

The uniqueness of this experience lies in the fact that the Bank of Italy not only provides a space for testing Fintech products/services shortly before market entry (sandbox) but also engages with the company in the earlier stages of idea development (Fintech Channel) and its concrete project implementation (Milan Hub). Additionally, this is a rather complex sandbox model, involving multiple public entities and a specific governance structure established by law (Ministry of Economy, Supervisory Authority, ad hoc Committee, etc.).

Another sector particularly suitable for this type of experimentation due to its extreme transversality and close connection with new technologies is the regulation of personal data processing[19]. In this case, the leading role is played by national data protection authorities. Of particular importance in the privacy sector are the English and Norwegian experiences.

In the United Kingdom, a sandbox focused on personal data protection has been created to explore new technologies (e.g., voice biometrics and facial recognition technology)[20]. This tool was developed by the Information Commissioner's Office (ICO)[21] to support companies developing products and services that use personal data in innovative and secure ways. The ICO's stated goal is to provide free assistance to businesses by offering advice on risk reduction and integration of "data protection by design", ensuring a better understanding of data protection frameworks and their impact on business activities.

The areas of greatest interest for the use of sandboxes include: (i) emerging technologies, such as hardware for augmented reality and other immersive technologies; (ii) biometric technologies, such as the face or voice authentication systems; (iii) exceptional innovations, a catch-all category for hypotheses that do not fit the previous categories but still present an exceptional level of innovation. It is explicitly stated that the feedback provided by the ICO cannot be considered a guarantee of compliance with data protection regulations[22].

Based on the English model, Norway[23] has also developed a sandbox by the Norwegian Data Protection Authority, with a particular focus on the intersection of privacy and artificial intelligence[24]. This sandbox is open to both public and private companies of different types, sectors, and sizes, intending to develop or having already developed AI systems with significant privacy implications. The projects must be relevant and impact a significant number of individuals, potentially benefiting from sandbox participation due to complex privacy implications (e.g., AI technology applied to biometrics). The duration of the sandbox can range from 3 to 6 months depending on the specific case, and each actor can collaborate with the authority in

ficiency of the financial system (e.g., lower costs or reduced resource utilization for the system), for the effective application of banking sector regulation (e.g., streamlining internal processes), or for better risk management of intermediaries (e.g., cost optimization); (3) the product/service must be in a sufficiently advanced state for experimentation, meaning it must be ready to start the experimentation immediately after receiving the admission notification to the sandbox; (4) the company must demonstrate that the activity to be tested is economically sustainable and has adequate financial coverage that extends throughout the experimentation period. Regarding the derogations applicable during the experimentation, it is provided that the Authorities may derogate from supervisory guidelines, regulations, or other acts of a general nature issued by them in the exercise of their functions (e.g., capital requirements; informational obligations; admissible company forms; any financial guarantees), but not from primary legislation or non-derogable EU rules. Cf. Bank of Italy official webpage.

19. For a more detailed analysis see Malgieri 2019.
20. Further information is available at ICO's official webpage.
21. The ICO is the UK's independent body set up to uphold information rights. The Department for Science, Innovation and Technology (DSIT) is the ICO's sponsoring department within Government.
22. In the document titled *Sandbox Terms and Conditions*, point 1.9 expressly provides that: «Any Feedback is given without prejudice to any decision or action that we may take in the future, including any enforcement or other regulatory action. The positions reflected in the Feedback may change over time, for example on receipt of further information by us, or following a change in law, court judgments, regulatory guidance or ICO policy».
23. Further information is available on the Norwegian Data Protection Agency's official webpage.
24. Further information about AI application of sandboxes available at Fenwick-Vermeulen-Corrales 2018. About the importance of regulating AI see Smuha 2021.

preparing a personalized individual project orientation plan[25]. The peculiarity lies in the fact that the admission application is evaluated not only by the Norwegian Data Protection Authority but also by an external reference group whose purpose is to provide a focused assessment specifically on the project's potential social benefit.

The goal of the sandbox is to benefit society by helping companies develop innovative AI technology that is ethical and responsible from a data protection perspective, compliant with legal requirements and fundamental rights. This objective is pursued based on three fundamental principles[26]: (a) lawful, ensuring compliance with applicable legislation; (b) ethical, adhering to generally recognized ethical principles and values; and (c) security, ensuring the robustness of the space and defence against cyber-attacks.

Regarding the first element (lawful), it is crucial to specify that in this case, the agency acts solely as a qualified consultant to the operator concerning GDPR compliance and relevant national regulations, without granting derogations during experimentation or implementing corrective measures. As for the second element (ethical), the focus is primarily on principles of fairness, transparency, and explainability applied to AI technology. The end user of the product/service under experimentation must be informed whether a machine has performed a specific operation involving their data and should be able to understand how their data is utilized and the corresponding outcomes. Moreover, the sandbox also requires the traceability of AI technology to enable potential audits and a concrete interpretation of the decision-making process in each specific case. Lastly, the third element (security) implies that the AI solution must be technically robust, not only for data protection purposes but also for accuracy and reliability, allowing for verifiability[27].

In concluding the analysis of national use cases, it is necessary to at least mention the German experience, whose peculiarity lies in the particular systematic approach it has devoted to the sandbox system. Germany, being a federal state, has chosen to develop a comprehensive national strategy for regulatory experimentation. Specifically, the German Federal Ministry of Economic Affairs (*BMWi*) acted by drafting a guide both for the use of regulatory sandboxes[28], in order to encourage their adoption and spread awareness, and for the provision of experimentation clauses[29], allowing each state (*Länder*) to introduce its own provisions and derogations. This systematic approach at the European level is unique in its kind, with the declared goal of incentivizing innovation policies to improve the utilization and regulation of technology in the interest of the entire civil society.

4. A (first) European-level initiative: the Artificial Intelligence Act and the Spanish Regulatory Sandbox on Artificial Intelligence

The technology sector which has gained the most exponential attention around the sandbox tool is undoubtedly artificial intelligence. The debate on the subject has intensified, particularly about the

25. In particular, the sandbox can provide the following types of activities to the experimenting company: (a) assistance with the implementation of privacy impact assessments (DPIA) and identification of privacy issues; (b) providing input on current technical and legal solutions to privacy challenges; (c) exploring opportunities for implementing integrated privacy; (d) conducting an informal site visit to highlight potential requirements; (e) offering a space for knowledge transfer and networking with other sandbox participants, external experts, and other authorities.
26. The fundamental principles are drawn from High-Level Expert Group on AI 2019.
27. Responsible and reliable artificial intelligence principles are analysed in more detail in Chapter 5 of the *Norwegian National Strategy for AI*.
28. See the web page of Federal Ministry for Economic Affairs and Energy (BMWi) *Making space for innovation. The handbook for regulatory sandboxes*, 2019.
29. See the Guide of the Federal Ministry for Economic Affairs and Energy (BMWi) *New flexibility for innovation. Guide for formulating experimentation clauses*, 2020.

new proposed regulation called the "Artificial Intelligence Act"[30] (AI Act), which is still ongoing[31] and currently in the "trilogue" phase[32]. As widely known, the AI Act is the first European legislative proposal that establishes a comprehensive and uniform framework dedicated to AI systems. More, the AI Act is also the first proposal that expressly includes regulatory sandboxes among possible regulatory solutions for AI technology, positioning them under the «Specific measures to support innovation» section (Title V) and dedicating three articles to them (53-54-55)[33].

The AI Act's objective is to ensure that there are regulatory facilitations in the field of artificial intelligence that provide flexibility to regulations and do not stifle innovation. The proposal does not specifically regulate the functioning of sandboxes, deferring the details to be established in delegated acts during the implementation phase of the legislation once approved. However, it already provides the legal basis for these experiments and offers initial reflections on their potential limitations and elements.

In particular, Article 53 of the AI Act (original text from the Commission of April 2021) explicitly encourages Member States to establish national regulatory sandboxes. It requests the Commission to set uniform rules for their implementation at the European level and outlines the general characteristics of sandboxes (controlled environment, facilitation of innovation, time-limited experimentation, autonomous responsibility of operators concerning their products). It also emphasizes the close connection with privacy matters. Furthermore, Article 54 provides the special legal basis for data processing related to AI sandboxes and Article 55 explicitly states that SMEs and start-ups should have priority access to the experiments.

Even from the original text of the AI Act, the intention to confer European-level recognition to the sandbox tool is evident. This aspect is even more pronounced in light of the amendments to the articles dedicated to sandboxes proposed by the Council and the Parliament[34].

Firstly, in the amended text by the Council and the Parliament, the sandbox is explicitly institutionalized, with each Member State being required to establish a regulatory sandbox on AI at the national level. Additionally, the establishment of sandboxes at the local, regional, and European levels is strongly encouraged (cf. Article 53 new paragraphs 1, 1a, and 1b). Secondly, the objectives of the sandbox are specified (providing guidance for compliance with the AI Act, facilitating experimentation and development of innovative solutions, and promoting normative learning in a controlled environment), with particular attention

30. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206, 21 April 2021. As this is a regulation proposal that is still subject to negotiations, unless otherwise specified, in this text, we will refer to this original Commission proposal.

31. The proposal for the AI Act put forward by the Commission is currently being debated by the EU co-legislators: the European Parliament and the Council. The content of the AI Act as finally adopted by the co-legislators may therefore differ from the text that is discussed herein. Unless explicitly stated otherwise, all references to the AI Act in this paper shall be understood as references solely to the proposal by the Commission. The European Parliament and the Council adopted their negotiating position on the AI Act respectively on 14 June 2023 (cf. P9_TA(2023)0236) and on 6 December 2022 (doc. 15698/22 – so-called *General Approach*).

32. In the context of the ordinary legislative procedure of the European Union, a "trilogue" is an informal interinstitutional negotiation that brings together representatives of the European Parliament, the Council of the European Union, and the European Commission. The aim of a trilogue is to reach a provisional agreement on a legislative proposal acceptable to both the Parliament and the Council, the co-legislators. This provisional agreement must then be adopted through each institution's formal procedures. A trilogue can take place at any stage of the legislative procedure with the objective of resolving outstanding issues and is chaired by the co-legislator hosting the meeting. The role of the Commission is to mediate between the parties. The timeline of the AI Act proposal is available at EUR-Lex (procedure 2021/106/COD).

33. Among the emerging pieces of literature on the AI Act, see: Mazzini-Scalzo 2023; Edwards 2022; Floridi 2021; De Gregorio-Dunn 2022.

34. See note 31.

to protecting fundamental rights during experimentation (cf. Article 53 new paragraphs 1d and 1e). Thirdly, for high-risk AI systems only, the institutional authorities of the sandbox must collaborate with the providers so that AI systems, once the experimentation period is complete, are presumptively considered compliant with the regulation (cf. Article 53 new paragraph 1f). This latter aspect represents a significant innovation as participation in the sandbox normally does not imply any presumption of regulatory compliance and underscores the high level of trust placed in this tool by European institutions[35]. Fourthly, a specific framework is introduced to define the governance relationships between sandboxes and AI offices, structuring European-level coordination with the European Commission at its helm (cf. Article 53 new paragraphs 5, 5a, and 6). This aspect highlights the regulator's intention to create a sandbox with a European structure.

Regardless of the final text of the proposal[36], it is certain that the AI Act, for the first time, establishes a unified institutional channel for qualified dialogue between the regulator and regulated entities through the sandbox tool, aiming to ensure flexible and future-proof regulation that fosters innovative AI systems. In this context, the initiative of the Spanish government is of great importance[37]. In June 2022, in partnership with the European Commission, Spain launched a project[38] of an AI-themed sandbox aimed at testing high-risk AI systems (HRAIS) and general-purpose AI systems (GPAIS)[39] in light of the AI Act proposal: the "Spanish Regulatory Sandbox on Artificial Intelligence" (hereinafter "Spanish pilot"). Compared to the previously analysed national experiences, the Spanish pilot has significant merit: it presents the first attempt at a pan-European system of the regulatory sandbox. The experimentation was open from the start to the participation of any Member

35. In particular the Article 53 new paragraph 1f proposed in the final text of the Parliament (Amendment No. 496) provides that: «Establishing authorities shall provide sandbox prospective providers who develop high-risk AI systems with guidance and supervision on how to fulfil the requirements set out in this Regulation, so that the AI systems may exit the sandbox being in presumption of conformity with the specific requirements of this Regulation that were assessed within the sandbox. Insofar as the AI system complies with the requirements when exiting the sandbox, it shall be presumed to be in conformity with this regulation. In this regard, the exit reports created by the establishing authority shall be taken into account by market surveillance authorities or notified bodies, as applicable, in the context of conformity assessment procedures or market surveillance checks».
36. Indeed, the significant innovations introduced by the Council and Parliament's amendments have raised debates on sandboxes during the trilogues. Specifically, according to recent rumours, the debate is currently between the Parliament, which advocates for the mandatory establishment of an AI-themed sandbox in each Member State, and the Council, which prefers to maintain it as a mere optional possibility. Additionally, unlike the Council's stance, the Parliament's position also includes providing AI developers who complete a sandbox with a presumption of conformity for their systems. Cf. EU Council sets path for innovation measures in AI Act's negotiations, in Euractiv, 10 July 2023.
37. The Spanish Secretary of State for Digitalisation and Artificial Intelligence - Spain's Ministry of Economic Affairs and Digital Transformation (SEDIA) is in charge of this.
38. Cf. information about the *Launch event for the Spanish Regulatory Sandbox on Artificial Intelligence*.
39. "High-risk AI systems" are regulated under Title III of the AI Act, and due to their "intrinsic dangerousness", they require a particularly complex and burdensome conformity assessment by the provider before being placed on the market. "General-purpose AI systems", on the other hand, are AI systems intended to perform functions of general application (e.g., image and speech recognition, audio and video generation, question answering, etc.) that can be used in multiple contexts and integrated into various other AI systems. In the original text of the Commission, GPAIS were largely ignored, while the Council's amending text (see note 39) dedicates an entire title to them (new Title Ia called "General Purpose AI Systems"), and Article 3(1b) defines them as follows: «'general purpose AI system' means an AI system that – irrespective of how it is placed on the market or put into service, including as open source software – is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems».

State that wished to join, and the results achieved will be made available to the entire European community. Additionally, an Expert Group was specifically established, serving both as the main forum to inform and involve all interested Member States in the pilot's developments and as a coordination centre, collecting all issues and concerns related to national sandboxes of various countries.

The pilot has multiple ambitious objectives: (1) clarifying the concrete compliance requirements of the AI Act regarding HRAIS and GPAIS; (2) transferring the compliance know-how developed during the pilot to companies; (3) enabling the development of innovative and reliable AI systems; (4) building skills and competencies within the national AI supervisory authority[40]; (5) providing practical learning experiences to support the development of standards and guidelines at the European level; and (6) increasing synergies and ensuring consistency with existing sectoral sandboxes at the national level (e.g., finance, automotive).

From a practical perspective, the pilot provides companies with both educational services on AI topics by qualified experts and personalized consultancy (through workshops and seminars) aimed at ensuring compliance with the AI Act. Structurally, the pilot is divided into two parallel and interconnected focus groups. The first focus group is dedicated to the practical execution of the sandbox, meaning the concrete testing of solutions and their compliance with the requirements of the AI Act. It manages the public call for companies (eligibility and selection criteria) and oversees the entire sandbox cycle. The main purpose is to assist businesses in testing and achieving compliance with the AI Act's requirements for HRAIS and GPAIS in practice[41]. The second focus group, on the other hand, takes a more theoretical-analytical approach and focuses on preparing and drafting documentation to support the sandbox. It absorbs the know-how from the pilot and develops guidelines, standards, and other tools that could be used by operators (public or private) in the future. For this reason, it includes a variety of experts, including academics, working to identify and propose how the requirements for HRAIS and GPAIS compliance should be implemented in practice[42]. The outcome of the two groups' work should result in a qualified synthesis of all the test results, proving compliance with the AI Act, documented in a publicly accessible report that can be used by all stakeholders.

By organizers' admission, the successful outcome of the sandbox depends not only on its proper structure but, above all, on the proactive collaboration of participating companies, whose feedback will be crucial for the final guidelines, the Commission's enforcement work, and improving the pilot's open call. To this end, the pilot participants will be subject to certain obligations: (a) they must conduct a compliance assessment in light of the AI Act; (b) they must ensure post-monitoring of their AI system for a defined period; (c) they must formally commit to collaborating and submitting reports to the pilot's coordination committee.

The Spanish pilot is expected to last three years and continue until 2025. The Spanish government and the Commission are working on the first open call, which should focus solely on HRAIS projects for a three-month experimentation period. The call is expected to include a limited number of companies, not exceeding 10-12, different in size (large, medium, SMEs, start-ups), business sector, and applied technology. Military and national security AI systems are excluded from the experimentation.

40. Not by chance, Spain is the first EU Member State to have introduced a national surveillance AI authority.

41. The priorities of the first focus group are as follows: (a) prepare the open call for companies interested in participating in the sandbox; (b) engage in ongoing dialogue with the participants of the sandbox throughout the experimentation process, guiding them in developing AI systems that comply with the future AI Act; (c) generate valuable know-how on the implementation of compliance requirements with the regulations and optimize them for future open calls; (d) compile a final report evaluating the experimentation and the achieved results.

42. The priorities of the second focus group are as follows: (a) establish a policy sandbox framework; (b) develop guidelines for both public and private entities to implement the requirements of the AI Act, gathering use cases and best practices; (c) propose audit scenarios for the competent authorities responsible for supervising AI systems during the sandbox period and in post-controls; (d) compile a final report on the sandbox's outcomes to be made public, thereby disseminating the acquired know-how and best practices during the pilot project's experimentation phase.

In conclusion, it is worth mentioning that in February 2023, the Commission presented the first true European-level sandbox, which will focus on blockchain technology and innovative use cases involving Distributed Ledger Technologies (DLT). It will be called the "European Blockchain Regulatory Sandbox"[43]. Unlike the Spanish pilot, this sandbox will be entirely managed at the European level by the Commission, in partnership with a consortium of qualified private entities in the blockchain field selected through a public call. It will last for three years and experiment with 20 blockchain technology-based projects each year. With this latest initiative as well, it is evident that the AI Act and the Spanish pilot have paved the way for the European consecration of the sandbox tool, and it is expected that the "European Blockchain Regulatory Sandbox" will be the first of many European technology-themed sandboxes.

5. The Cybersecurity implications: the Cyber Resilience Act and future perspectives

The themes of cybersecurity and artificial intelligence are closely interconnected, as emphasized by the AI Act, which requires an adequate level of cybersecurity as one of the compliance conditions for high-risk AI systems (cf. Recital 49; Articles 13 and 15)[44]. Therefore, any AI-focused sandbox, including the Spanish pilot, must also consider cybersecurity aspects to experiment with AI systems that comply with the AI Act.

Like artificial intelligence, cybersecurity has gained significant importance at the European level recently. In alignment with the EU Cybersecurity Strategy Digital Decade[45], several significant new regulations have been proposed in this field, such as the Cybersecurity Act[46], the new NIS2 Directive[47], the Cyber Resilience Act[48], and the Cyber Solidarity Act[49]. Hence, companies find themselves increasingly confronted with numerous new rules and compliance obligations also in the cybersecurity domain. In this context, the proposed "Cyber Resilience Act" (CRA), currently undergoing negotiation between European co-legislators, holds particular relevance[50].

The CRA proposal has been deemed necessary due to the cross-border nature of digital products and cyber-attacks affecting them. Currently, most hardware and software products lack any uniform legislation ensuring their cybersecurity, and no regulation addresses the cybersecurity of non-embedded software, which represents a critical vul-

43. Further details about the *Launch of the European Blockchain Regulatory Sandbox* are available at *Shaping Europe's digital future* website.
44. Article 15(1) AI Act: «High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle».
45. Further details are available at *Shaping Europe's digital future* website.
46. Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification COM(2017) 477, 13 September 2017.
47. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
48. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454, 15 September 2022. Further details about the proposal are available at *Shaping Europe's digital future* website. Again, as with the AI Act proposal, since this is still an ongoing proposal, we will refer to the European Commission's original text dated 15 September 2022 unless otherwise indicated.
49. Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (still ongoing), COM(2023) 209, 18 April 2023.
50. For updates regarding the timeline of the proposal please refer to *European Parliament, Legislative Train Schedule*.

nerability in the era of digital products[51]. Therefore, the CRA aims to introduce a horizontal regulatory framework at the European level, establishing comprehensive and uniform cybersecurity requirements for all «products with digital elements» (defined in Article 3, No. 1 of the CRA)[52] entering the European internal market.

The proposal seeks to address two key issues: (a) the widespread low level of cybersecurity of digital products in the European single market, and (b) inadequate understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties and/or using them securely. To achieve these goals, the proposal acts on two fronts: it requires manufacturers to enhance the cybersecurity of digital products from the design and development phase throughout their lifecycle while ensuring that businesses and consumers can use products with digital elements safely.

The CRA establishes specific obligations for economic operators throughout the production chain (manufacturers, distributors, importers) concerning the entry of products with digital elements into the market, tailored to their roles and responsibilities. These obligations include subjecting all digital products to a detailed conformity assessment procedure, divided into specific steps (conformity assessment, declaration of conformity registration, CE marking[53], and maintenance of technical documentation). Following this process, products can enter the market only when properly provided, installed, maintained, and used for their intended purpose (cf. Article 5 and 24 of the CRA; see also Annex I), and thus considered "cyber-safe"[54]. It is essential to highlight that the CRA's conformity assessment procedure applies a risk-based approach, varying in intensity and detail based on the criticality associated with each product (cf. Article 6), similar to the approach adopted by the AI Act[55].

While primarily the responsibility of the manufacturer, the conformity assessment procedure is overseen by surveillance and control bodies. The proposal establishes a system of conformity assessment bodies (so-called notified bodies) responsible for ensuring a high level of cybersecurity and trust for all stakeholders. Additionally, the CRA stipulates that each member state appoints a notification authority responsible for the necessary pro-

51. For a detailed overview of the CRA proposal see also: Eckhardt-Kotovskaia 2023; Nuthi 2022; Chiara 2022.

52. Article 3 No. 1 CRA: «'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately». In essence, the proposal applies to products with digital elements whose intended use or reasonably foreseeable use involves a direct or indirect logical or physical connection to a device or network. It does not apply to products for which cybersecurity requirements are already established in existing EU regulations, such as medical devices, aviation, or vehicles.

53. Article 3 No. 32 CRA: «'CE marking' means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing».

54. In essence, the proposal establishes: (i) rules for placing products with digital elements on the market to ensure their cybersecurity; (ii) essential requirements for the design, development, and production of products with digital elements, and obligations for economic operators concerning the cybersecurity of these products; (iii) essential requirements for vulnerability management processes implemented by manufacturers to ensure the cybersecurity of products with digital elements throughout their entire lifecycle, and obligations for economic operators concerning these processes; (iv) rules regarding market surveillance and the enforcement of the aforementioned rules and requirements.

55. Following the approach envisaged in the AI Act proposal concerning high-risk AI systems, the CRA regulation proposal also includes specific provisions for "critical products with digital elements". These products are subject to distinct and stricter conformity assessment procedures, and, as indicated in Annex III, they are categorized into two different classes (Class I and Class II) based on the level of cybersecurity risk they pose (Class II representing a higher risk).

cedures concerning the assessment, notification, and monitoring of notified bodies, along with a dedicated market surveillance authority endowed with appropriate corrective and sanctioning powers (cf. Article 47).

Clear similarities exist between the CRA and the AI Act. Both proposals (i) aim to ensure the safety and reliability of digital technologies in the internal market; (ii) impose compliance requirements and obligations on companies developing digital products through a risk-based approach; (iii) require special attention to the protection of personal data; (iv) seek to bolster consumer confidence in using digital technologies; and (v) give particular consideration to SMEs and their compliance costs.

The CRA further emphasises the connection between the two regulations when it addresses "products with digital elements classified as high-risk AI systems" (cf. Article 8). Article 8 of the CRA indeed provides a presumption of conformity to the CRA for this specific type of product if they comply with the cybersecurity requirements outlined in Article 15 of the AI Act (except for "critical products with digital elements"). Moreover, Article 41(10) of the CRA also states that for "products with digital elements classified as high-risk AI systems", the market surveillance authorities designated under the AI Act are also responsible for compliance with the CRA, thereby clearly highlighting the overlap between the two regulations.

Despite these connections and similarities, unlike the AI Act, the original text of the CRA does not refer to the instrument of regulatory sandboxes. The question naturally arises, given that both proposals include a conformity procedure for complex technological products.

The reasons for this omission could be varied. It is possible that the Commission decided in this way because due to the different scope of application of the two regulations. Indeed, the AI Act focuses on a narrower subject (AI systems) compared to the CRA (all products with digital elements), and this aspect might have led the regulator to avoid opening up a category of products that is too broad for the sandbox instrument. Another reason might be related to the different application domains of the two proposals. Sandboxes represent relatively "new" hybrid regulatory tools, and the cybersecurity theme is particularly delicate and relevant to the "European system", as it is closely connected to national security aspects. Hence, an additional period of specific study and evaluation may be required to verify the practical utility of sandboxes in this sector. In this sense, the Spanish pilot will undoubtedly play a fundamental role and serve as a crucial testing ground, especially considering its focus on cybersecurity elements for high-risk systems (cf. Article 15 AI Act)[56].

Nevertheless, the CRA is still ongoing, and it cannot be excluded that during the negotiations, a modification will be proposed to explicitly introduce the instrument of sandboxes. In this regard, it is important to underline that the text presented by the ITRE Parliamentary Committee (May 2023)[57] suggests a new recital (69a)[58] and a new Article

56. Indeed, it is not surprising that the Spanish government also involved the Spanish national cybersecurity agency (INCIBE) in the pilot of the AI-themed sandbox.

57. ITRE (Committee on Industry, Research and Energy) is the parliamentary committee responsible for managing the proposal within the European Parliament. Cf. European Parliament, Legislative Observatoruy, procedure 2022/272 (COD).

58. In particular, amendment No. 201 proposed in ITRE's draft text introduces a New Recital No. 69a that reads as follows: «Economic operators that are SMEs, with particular attention paid to micro enterprises and start-ups, should be provided with dedicated guidance and where possible with financial support to adapt to the requirements of this Regulation when placing new product on the market. In particular, the Commission, ENISA and the Member States, should establish a European cyber resilience regulatory sandboxes, the Commission should establish a special webpage and provide direct tailored advice, and streamline the financial support from Digital Europe Programme and other relevant EU programmes. Member States should consider all possible complementary actions aiming at advice and financial support for SMEs, including via digital/cybersecurity hubs and start-up accelerators. Where the market surveillance authorities exercise their supervisory enforcement tasks, they should take into consideration whether the manufacturer is a SME, with particular attention payed to micro companies and start-ups». Full text of the draft is available at European Parliament website.

(49a)[59] encouraging the Commission, the European Union Agency for Cybersecurity (ENISA), and Member States to establish "European cyber resilience regulatory sandboxes". This first text was followed by an official "Report" (July 2023)[60] confirming the Parliament's willingness to invest in the regulatory sandbox tool in the area of cybersecurity.

In particular, the position of the Parliament (new Article 53a[61]) is to recommend creating free experimentation spaces dedicated to companies - with a particular focus on SMEs and start-ups - to help them comply with the requirements of the proposal and expressly establishes the creation of sandboxes at the European level aimed at: (a) providing a controlled environment that facilitates the development, testing and validation of products with digital elements before their placement on the market; (b) providing practical support to economic operators, including via guidelines and best practices; (c) contributing to evidence-based regulatory learning.

The co-legislators started trilogue negotiations on 27 September 2023 and the intention seems to be to close a political agreement by the first quarter of 2024.

In any case, even if the CRA's text were to remain in its original version, this would not prevent the provision of cybersecurity-related sandboxes to support companies developing products with digital elements, thus complying with the CRA's required procedure before introducing them to the market. The utility served by the Spanish pilot, in terms of structuring guidelines to improve the enforcement of the AI Act, could also be identified in a sandbox operating with the same purpose in the context of the CRA. There are no obstacles in this regard; in fact, some experimentation spaces dedicated to cybersecurity product development already exist in the European landscape and can be used as a foundation for proposing new ones[62].

Furthermore, the fact that the Council and the Parliament amended the AI Act, explicitly requiring the structuring of a national sandbox dedicated to AI, may be seen as an opportunity to reflect on the possibility of developing a system of interconnected national sandboxes focused on cybersecurity as well. These sandboxes could be aimed at testing compliance with the CRA for products with digital elements, whether they integrate AI systems or not. One proposal could be to establish

59. In particular, Amendment No. 435 proposed in ITRE's draft text introduces a New Article49a titled "Cyber Resilience Regulatory Sandboxes" that reads as follows: «The Commission, ENISA and Member States shall establish a European cyber resilience regulatory sandboxes with voluntary participation of manufacturers of products with digital elements to: (a) provide for a controlled environment that facilitates the development, testing and validation of the design, development and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan; (b) provide practical support to economic operators, in the first place to SME's, with particular attention paid to micro-enterprises and start-ups, including via guidelines and best practices to comply with the essential requirements set out in Annex I; (c) contribute to evidence-based regulatory learning». Full text of the draft is available at European Parliament website.

60. European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (doc. A9-253/2023).

61. In particular, amendment No. 163 proposed in Report's text introduces a new Article 53a titled *Regulatory Sandboxes* that reads as follows: «The Commission and ENISA, may establish a European regulatory sandbox with voluntary participation of manufacturers of products with digital elements to: (a) provide for a controlled environment that facilitates the development, testing and validation of the design, development and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan; (b) provide practical support to economic operators, including via guidelines and best practices to comply with the essential requirements set out in Annex I; (c) contribute to evidence-based regulatory learning».

62. These include the *European Digital Innovation Hubs* (EDIHs), launched by the European Cyber Security Organisation (ECSO), which aim to provide businesses and professionals with a safe and secure environment in which to test innovative cyber security solutions. We also could mention the *Cyber Lab*, developed by the UK's National Cyber Security Centre (NCSC), which allows companies to test innovative cyber security solutions in a controlled and protected environment, supervised by the industry regulator.

a national cybersecurity-focused sandbox within the national supervisory authority required by the CRA to be nominated by each Member State (cf. Article 41(2))[63]. In this regard, the Spanish pilot and other European experiences would certainly represent excellent best practices from which to learn the most effective method of structuring a sandbox and the best techniques to initiate a constructive dialogue on AI and cybersecurity at the European level.

In substance, AI Act and CRA share the basic concept (and the legal basis of Article 114 TFEU) that regulation of technology must first and foremost ensure a safe European internal market. The approach of both proposals to regulate the product (AI systems and products with digital elements) makes the application of the regulatory sandbox tool particularly favorable and useful, allowing companies and authorities to ensure, in collaboration and through a continuous qualified dialogue, the placing on the market of products that are both innovative and safe. The choice of the European regulator to bet on the sandbox tool is clear in the field of artificial intelligence, as can be seen in the light of both the AI Act discipline and the activation of experiments at the European level (Spanish pilot and European Blockchain Regulatory Sandbox). There are no obstacles to the same kind of reasoning being applied to CRA and the related need to introduce only 'cyber-safe' digital products on the market.

In conclusion, the path identified by the European regulator appears to be quite clear: new technologies demand new regulatory tools, and regulatory sandboxes certainly embody this new philosophy. A critical theme like cybersecurity cannot be excluded from such experimentation, as it represents a central topic, just like AI, in shaping a healthy, fair, and safe digital environment. Furthermore, companies operating in the digital product sector (even those not connected to AI systems) deserve the opportunity to benefit from experimentation spaces to enhance their production capabilities. The hope is that the Spanish pilot will achieve great success and pave the way for the creation of other European-level sandboxes dedicated to CRA compliance and cybersecurity themes in general, thus establishing a virtuous framework for regulatory experimentation at the European level. This would enable the European digital market to remain at the forefront of innovation while ensuring safety and security. In this regard, the recent decision of the Spanish government (November 2023) to establish by national law a controlled testing environment for assessing compliance with the AI Act suggests that the direction taken is to strongly invest in the regulatory sandbox tool in the coming future[64].

It is very recent news (1 December 2023) that the two co-legislators just reached a political agreement on CRA[65]. The agreement is now subject to formal approval by both the European Parliament and the Council and, once adopted, the CRA will enter into force on the 20th day following its publication in the Official Journal.

We have to wait until then to see whether the final text will include an explicit reference to the regulatory sandboxes tools or whether it will remain silent. Either way, the horizon remains open for future experimental regulatory spaces in the field of cybersecurity.

References

H.J. Allen (2019), *Regulatory Sandboxes*, in "George Washington Law Review", vol. 87, 2019, n. 3

A. Attrey, A.M. Lesher, C. Lomax (2020), *The role of sandboxes in promoting flexibility and innovation in the digital age*, OECD Going Digital Toolkit Policy Note N. 2, 2020

63. Article 41(2) CRA: «Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation».

64. Cf. Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

65. Cf. *Political agreement on Cyber Resilience Act*, 2023.

R. Baldwin (2005), *Is better regulation smarter regulation?*, in "Public Law", 2005

L. Bennett Moses (2013), *How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*, in "Law, Innovation & Technology", vol. 5, 2013, n. 1

L. Bromberg, A. Godwin, I. Ramsay (2017), *Fintech Sandboxes: Achieving a Balance between Regulation and Innovation*, in "Journal of Banking and Finance Law and Practice", vol. 28, 2017, n. 4

R.P. Buckley, D. Arner, R. Veidt, D. Zetzsche (2020), *Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond*, in "Washington University Journal of Law & Policy", 2020, vol. 61

P.G. Chiara (2022), *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in "International Cybersecurity Law Review", 2022, n. 3

G. De Gregorio, P. Dunn (2022), *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in "Common Market Law Review", vol. 59, 2022, n. 2

P. Eckhardt, A. Kotovskaia (2023), *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in "International Cybersecurity Law Review", 2023, n. 4

L. Edwards (2022), *The EU AI Act proposal*, Ada Lovelace Institute, 2022

European Banking Authority (2019), *Report FinTech: Regulatory sandboxes and innovation hubs*, 2019

European Commission (2023), *'Better regulation' toolbox,* July 2023 edition

European Parliament (2020), *Regulatory Sandboxes and Innovation Hubs for FinTech Impact on innovation, financial stability and supervisory convergence*, Study for the committee on Economic and Monetary Affairs, Author R. Parenti, 2020

M. Fenwick, E.P.M. Vermeulen, M. Corrales (2018), *Business and Regulatory Responses to Artificial Intelligence: Dynamic Regulation, Innovation Ecosystems and the Strategic Management of Disruptive Technology*, in M. Corrales, M. Fenwick, N. Forgó (eds.), "Robotics, AI and the Future of Law", Springer, 2018

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

M.A. Heldeweg (2015), *Experimental legislation concerning technological & governance innovation – An analytical approach*, in "The Theory and Practice of Legislation", vol. 3, 2015, n 2

T.F.. Hellmann, A. Montag, N. Vulkan (2022), *The Impact of the Regulatory Sandbox on the FinTech Industry*, 2022

High-Level Expert Group on AI (2019), *Ethics guidelines for trustworthy AI*, European Commission, 2019

G. Malgieri (2019), *Automated Decision-Making in the EU Member States. The right to Explanation and other "suitable safeguards" for Algorithmic Decisions in the EU National Legislations*, in "Computer Law & Security", vol. 35, 2019, n. 5

G. Mazzini, S. Scalzo (2023), *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. Camardi (a cura di), "La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche", 25-26 novembre 2021, Cedam, 2023

M. Mousmouti (2018), *Making Legislative Effectiveness an Operational Concept: Unfolding the Effectiveness Test as a Conceptual Tool for Lawmaking*, in "European Journal of Risk Regulation", vol. 9, 2018, n. 3

K. Nuthi (2022), *An Overview of the EU's Cyber Resilience Act*, Center for data and innovation, 26 September 2022

S.T. Omarova (2020), *Technology v Technocracy: Fintech as a Regulatory Challenge*, in "Journal of Financial Regulation", vol. 6, 2020, n. 1

C.M. Radaelli (2007), *Whither better regulation for the Lisbon agenda?*, in "Journal of European Public Policy", vol. 14, 2007, n. 2

S. Ranchordas (2021), *Experimental lawmaking in the EU: Regulatory Sandboxes*, University of Groningen Faculty of Law, Research Paper No. 12/2021, 22 October 2021

S. Ranchordas (2021a), *Experimental Regulations for AI: Sandboxes for Morals and Mores*, University of Groningen Faculty of Law Research Paper No. 7/2021, 2021

S. Ranchordas (2015), *Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation*, in "Jurimetrics", vol. 55, 2015, n. 2

N.A. Smuha (2021), *From a 'Race to AI' to a 'Race to AI Regulation' - Regulatory Competition for Artificial Intelligence*, in "Law, Innovation and Technology", vol. 13, 2021, n. 1

R. van Gestel, G. van Dick (2011), *Better Regulation through Experimental Legislation*, in "European Public Law", vol. 17, 2011, n. 3

M. Weimer, L. Marin (2016), *The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies*, in "European Journal of Risk Regulation", 2016, n. 3

J.B. Wiener (2006), *Better Regulation in Europe,* in "Current Legal Problems", vol. 59, 2006, n. 1

World Bank Group (2020), *Global Experiences from Regulatory Sandboxes. Finance, Competitiveness & Innovation Global Practice*, Fintech Note No. 8, 2020

K. Yordanova (2019), *The Shifting Sands of Regulatory Sandboxes for AI*, KU Leuven CiTiP Blog, 18 July 2019

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0115 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Gabriele Braccioni

Social network e pubblica amministrazione: criticità e best practice

Il presente lavoro costituisce il tentativo di individuare i molteplici aspetti critici connessi all'utilizzo dei social network da parte della pubblica amministrazione. Partendo dalla disciplina della comunicazione pubblica e dagli obblighi imposti dall'ordinamento agli enti pubblici, vengono analizzate le conseguenze giuridiche che si possono ripercuotere sull'ente e sul dipendente qualora l'utilizzo delle piattaforme di comunicazione non sia frutto di un'attenta analisi preventiva di compliance su numerosi aspetti spesso tralasciati, fornendo – in conclusione – alcune indicazioni operative o best practice.

Social network – Pubblica amministrazione – Comunicazione pubblica – Contratto – Responsabilità

Social networks and public administration: critical issues and best practices

This essay aims to identify the several critical aspects connected to the use of social networks by the public authorities. On the basis of the current legal framework concerning public communication and obligations imposed on public bodies, the legal consequences that may have repercussions on the bodies themselves and the employees will be analysed, considering that the use of communication platforms is not the result of a careful prior compliance analysis on numerous aspects that are often overlooked. Some operational indications about best practices will be provided in the conclusions.

Social network – Public administration – Public communication – Contract – Accountability

L'Autore è avvocato del foro di Urbino; si occupa di diritto delle nuove tecnologie

1. Il contesto normativo di riferimento: gli obblighi gravanti sulla PA

Il diritto all'informazione pubblica trova copertura costituzionale non solo nell'art. 97 Cost. e nel complesso delle altre norme costituzionali su cui si fonda il nostro ordinamento democratico (artt. 1, 2, 3 e 21 Cost.) ma anche 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"[1].

La normativa italiana ha risentito inoltre delle spinte sovranazionali, soprattutto provenienti dall'ordinamento dell'Unione europea, tese a ridisegnare l'organizzazione delle attività delle pubbliche amministrazioni in chiave digitale, il cui fine ultimo non è solamente il raggiungimento della digitalizzazione, ma anche quello di garantire una maggiore partecipazione e soddisfazione dei cittadini. Ciò ha determinato l'adozione di una serie di provvedimenti che hanno sancito il passaggio della comunicazione pubblica concepita come servizio avente carattere meramente strumentale a vera e propria funzione amministrativa.

La legge 7 giugno 2000, n. 150 recante la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni" è la prima legge-quadro sulla comunicazione pubblica con la quale il legislatore ha introdotto nell'ordinamento italiano precisi obblighi in capo alle amministrazioni indicate all'articolo 1, comma 2, del d.lgs. 3 febbraio 1993, n. 29[2].

1. Infatti si ritiene che non basti «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 artt. 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 repubblica (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)», Montagnani 2021, p. 110 e in particolare le osservazioni contenute alla nota 35.
2. Norma abrogata dall'articolo 72 del d.lgs. 30 marzo 2001, n. 165, ma la cui disciplina è riportata all'art. 1 comma 2 di quest'ultimo ai sensi del quale sono compresi anche tutti gli enti regionali.

La legge in esame ha introdotto diverse strutture e figure professionali all'interno delle PA, in particolare:

- l'ufficio relazioni con il pubblico per la gestione delle attività di comunicazione;
- l'ufficio stampa per le competenze relative alla comunicazione e divulgazione delle informazioni nei confronti dei media;
- il portavoce quale figura che supporta l'amministrazione pubblica nei rapporti di carattere politico-istituzionale con gli organi di informazione.

A tali soggetti, che devono essere forniti delle necessarie competenze in tema di comunicazione, l'ordinamento attribuisce il compito di gestire il delicato rapporto tra amministrazione e cittadino in maniera coerente con i principi di trasparenza[3] (che favorisce e promuove l'accountability), di partecipazione, di efficacia amministrativa nonché con quelli di digitalizzazione[4].

Anche la comunicazione pubblica, in quanto esercizio dell'attività istituzionale dei singoli enti, deve infatti rispettare e garantire i princìpi costituzionali di buon andamento e trasparenza, oltre che essere funzionale al raggiungimento della massima partecipazione dei cittadini all'amministrazione pubblica.

Una delle funzioni principali cui devono assolvere i soggetti che si occupano di relazioni con il pubblico è, infatti, la comunicazione esterna, ovvero trasferire e diffondere le informazioni e le comunicazioni verso i cittadini. L'utilizzo delle tecnologie informatiche e della rete Internet permette di innovare le attività e lo svolgimento dei procedimenti amministrativi, perseguendo gli obiettivi di efficacia, efficienza ed economicità; consente di aprire nuovi canali di comunicazione e nuovi spazi di partecipazione perseguendo gli obiettivi di trasparenza e democraticità; permette di ripensare e migliorare l'erogazione dei servizi pubblici aprendo nuove possibilità di contatto e offrendo nuovi servizi, al fine di semplificare i rapporti con i cittadini e con le imprese: in sintesi attraverso le tecnologie dell'informazione e della comunicazione è possibile realizzare un'amministrazione pubblica digitale[5], così auspicata da gran parte delle norme programmatiche recepite nel nostro ordinamento provenienti, spesso, da fonti ultra nazionali.

La pubblica amministrazione deve pertanto predisporre un piano di comunicazione che tenga conto oltre che dei contenuti da pubblicare – che saranno ovviamente legati alla funzione istituzionale di ogni singolo ente – anche di quanto previsto dall'ordinamento in ordine a:

- la tutela del diritto d'autore (l. 22 aprile 1941, n. 663);
- la disciplina delle attività di informazione e comunicazione delle pubbliche amministrazioni (l. 7 giugno 2000, n. 150);
- la normativa in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e Regolamento Ue n. 2016/679 - GDPR);
- le disposizioni per favore l'accesso dei soggetti disabili agli strumenti informatici (l. 9 gennaio 2004, n. 4);
- il Codice dell'amministrazione digitale (CAD) (d.lgs. 7 marzo 2005, n. 82);
- il nuovo Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36)[6].

Oltre alle norme sopra citate l'ordinamento italiano ha poi meglio specificato come raggiungere gli obbiettivi e rispettare i princìpi sopra enunciati con una serie di provvedimenti di rango secondario che hanno fornito maggiori dettagli, come ad esempio le *Linee guida per i siti web della PA* previste dall'art. 4 della direttiva n. 8 del 26 novembre 2009 del Ministero per la Pubblica Amministrazione e

3. Il cui fondamento normativo deve individuarsi nell'art. 1 della l. 7 agosto 1998, n. 241.
4. In attuazione dell'art. 3 del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) che prevede un vero e proprio diritto all'uso delle tecnologie da parte di cittadini e imprese nelle comunicazioni con i pubblici uffici.
5. L'espressione è utilizzata anche in FormezPA 2009.
6. Entrato in vigore il 1° aprile 2023, ha acquistato parzialmente efficacia dal 1° luglio 2023, termine fino al quale ha continuato ad applicarsi – *in toto* – il codice previgente di cui al d.lgs. 18 aprile 2016, n. 50. La piena applicazione del nuovo codice per gli aspetti legati alla digitalizzazione dell'ecosistema dei contratti sarà completa a partire dal 1° gennaio 2024.

l'Innovazione[7] successivamente aggiornate con le recenti *Linee guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione* adottate dall'Agenzia per l'Italia Digitale (AgID) con determinazione n. 224 del 26 luglio 2022[8]. A tali linee guida si accompagnano poi alcuni vademecum di approfondimento su singole tematiche verticali, come ad esempio il *Vademecum* "*Pubblica Amministrazione e social media*"[9] pubblicato da FormezPA[10] nel 2009 che fornisce importanti indicazioni sull'utilizzo della comunicazione attraverso i social network.

Va inoltre segnalato che con il "Decreto semplificazioni" (d.l. 16 luglio 2020, n. 76 convertito con la l. 11 settembre 2020, n. 120) il legislatore, nel fissare nuovi obiettivi per la pubblica amministrazione digitale, ha previsto 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 da soggetti privati. In particolare, al fine di semplificare e favorire l'accesso ai servizi in rete della pubblica amministrazione e l'effettivo esercizio del diritto all'uso delle tecnologie digitali, l'art. 24 del d.l. n. 76/2020 ha introdotto diverse modifiche agli artt. 3-*bis*, 6-*bis*, 6-*quater*, 64, 64-*bis*, e 65 del CAD.

Il legislatore ha voluto dare una spinta decisa all'utilizzo dell'identità digitale come modalità di accesso ai servizi offerti dalla PA[11]; inoltre, con l'introduzione dell'art. 6-*quater*, si è finalmente reso operativo il domicilio digitale per tutti i cittadini mediante l'istituzione dell'INAD (Indice nazionale dei domicili digitali)[12], ove chiunque può ora registrarsi e indicare il proprio domicilio digitale che verrà utilizzato dalla pubblica amministrazione per le comunicazioni ufficiali[13,14].

Da ultimo va anche tenuta in considerazione l'approvazione da parte del Parlamento europeo del Regolamento 19 ottobre 2022, n. 2022/2065 (*Digital Service Act*) con il quale, pur mantenendo l'impianto normativo già dettato con la Direttiva sul commercio elettronico 2000/31/CE, il legislatore comunitario ha inteso fornire maggiore tutela in relazione ai contenuti illegali, alla pubblicità trasparente e alla disinformazione nell'ambiente digitale[15].

7. Vedi direttiva n. 8/09 relativa alla riduzione dei siti web delle P.A. e per il miglioramento della qualità dei servizi e delle informazioni on line al cittadino.
8. Il cui testo è disponibile al link https://docs.italia.it/italia/design/lg-design-servizi-web/it/versione-corrente/index.html.
9. Cfr. FormezPA 2009.
10. Formez PA – Centro servizi, assistenza, studi e formazione per l'ammodernamento delle P.A. è un'associazione riconosciuta con personalità giuridica di diritto privato, *in house* alla Presidenza del Consiglio - Dipartimento della Funzione Pubblica ed alle Amministrazioni associate.
11. Escludendo che tale accesso possa avvenire tramite semplice PIN e rendendo obbligatoria l'identificazione a fattore multiplo come quella prevista per CIE, SPID o CNS.
12. La completa operatività dell'INAD si è avuta a partire dal 6 luglio 2023, data dalla quale è stata resa possibile la consultazione delle PEC indicate dai cittadini.
13. In precedenza solamente i cittadini facenti parte di alcune categorie professionali avevano la possibilità (*rectius* l'obbligo) di munirsi di PEC e di registrarsi in uno dei pubblici elenchi previsti dal CAD. D'ora in poi chiunque potrà registrare un indirizzo di posta elettronica certificata in un elenco pubblico valido per le comunicazioni e le notificazioni.
14. Altre importanti novità sono la previsione di una piattaforma che operi come strumento unico per la notifica digitale di tutti gli atti della pubblica amministrazione e alcuni interventi resisi necessari per armonizzare la legislazione interna in tema di formazione, gestione e conservazione dei documenti informatici con la disciplina europea.
15. Il DSA è destinato ad applicarsi a tutti i servizi intermediari che trasmettono o memorizzano informazioni, inclusi piattaforme, motori di ricerca e servizi di hosting, offerti a destinatari situati all'interno dell'Unione europea, ma per il momento è entrato in vigore esclusivamente per le grandi piattaforme, identificate come VLOP (*Very Large Online Platforms*) e VLOSE (*Very Large Online Search Engines*) secondo le definizioni della nuova regolamentazione mentre, per le altre piattaforme, l'applicazione delle disposizioni del DSA diventerà operativa entro febbraio 2024. Tale Regolamento potrebbe avere un impatto anche sui temi trattati nel presente

1.1. Il sito istituzionale

Nell'attuale assetto tecnologico e sociale del mondo contemporaneo, il primo elemento che pare soddisfare le esigenze di comunicazione della PA è senza dubbio il sito web istituzionale che rappresenta il vero *touch point* con cui l'amministrazione entra in contatto con i propri stakeholder.

Il sito deve contenere le informazioni previste come obbligatorie dall'ordinamento (c.d. albero della trasparenza) quali l'indirizzo della sede legale, la partita IVA (o codice fiscale) la PEC, i provvedimenti dei quali è obbligatoria la pubblicazione, la pubblicità legale, l'albo pretorio, la pianta organica, i nominativi degli amministratori, le procedure concorsuali e i bandi di gara etc. Molte di queste informazioni devono essere obbligatoriamente inserite in un'apposita sezione denominata "Amministrazione trasparente" che deve essere raggiungibile da tutte le pagine del sito[16].

Il sito deve altresì rispettare le norme che tendono a garantire l'accessibilità dei contenuti anche alle persone con disabilità, mediante accorgimenti tecnici che, in un approccio *by design*, dovrebbero essere implementati sin dalla fase di progettazione[17].

In definitiva il sito web rappresenta solamente una diversa modalità con cui l'amministrazione rende pubbliche le informazioni che, comunque, il cittadino avrebbe potuto reperire consultando i corrispondenti documenti cartacei. Il sito web, analogamente alla pubblicazione cartacea, è quindi una modalità di comunicazione statica che non prevede la compartecipazione degli utenti all'attività di divulgazione: il cittadino riceve le informazioni solamente se accede alla sezione corretta del sito, e lo farà solamente se mosso da un effettivo interesse a conoscere un determinato atto.

1.2. I social network

Il superamento del concetto di web statico e l'avvento del web 2.0, caratterizzato dall'utilizzo di piattaforme che coinvolgono l'utente in maniera molto più partecipata, ha profondamente cambiato lo scenario preesistente. A partire dalla metà del primo decennio degli anni 2000, la maggior parte degli utenti ha cominciato ad utilizzare in maniera prevalente le applicazioni che "girano" sul web le quali non necessitano di essere istallate sui dispositivi, in ciò agevolati anche dalla diffusione capillare dei dispositivi mobili potentissimi, in precedenza poco utilizzati.

In questo contesto hanno svolto la funzione di leader trascinatori del fenomeno le piattaforme social network come *Youtube*, *Facebook*, *Instagram* e *Twitter*. Tali servizi consistono in veri e propri ambienti di condivisione, «dove ogni forma di aggregazione (ludica, professionale o parentale) crea un valore infinito arricchendosi anche dei contenuti generati dagli utenti»[18] tanto da indurre a parlare di *web sociale* quale corrispettivo telematico della socialità e relazionalità tipica delle comunità.

L'elemento di novità è pertanto costituito dall'interazione tra gli utenti che ha generato l'interesse tra gli utilizzatori, tanto che tutti i servizi web nati negli ultimi dieci anni hanno considerato, sin dalla progettazione, l'elemento della condivisione come centrale rispetto al servizio offerto.

---

lavoro, in quanto applicandosi ai social network è possibile che la sua disciplina finisca per ripercuotersi sull'utilizzo degli account della pubblica amministrazione.

16. L'art. 9 del d.lgs. 14 marzo 2013, n. 33 prevede che la sezione "Amministrazione trasparente" sia visibile nella home page del sito, ma le best practice indicate (anche) dalle *Linee guida di design per i servizi digitali della PA*, nella versione pubblicata dall'AgID il 10 novembre 2022, al punto 2.4.2 suggeriscono di inserire tale sezione nel footer in quanto visualizzabile da tutte le pagine.
17. Le norme di riferimento sono contenute nei seguenti provvedimenti: l. 9 gennaio 2004, n. 4 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici"; d.lgs. 10 agosto 2018, n.106, attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici; d.m. 30 aprile 2008, "Regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili" (G.U. Serie Generale n. 136 del 12 giugno 2008); d.l. 18 ottobre 2012, n. 179, (convertito con modificazioni dalla l. 17 dicembre 2012, n. 221), all'art. 9 ("Documenti informatici, dati di tipo aperto e inclusione digitale"), nonché numerosi provvedimenti Ue che hanno disciplinato il tema dell'accessibilità.
18. Vedi FormezPA 2009.

La rete Internet è così diventata un luogo "da abitare", non più "da consumare" e i cittadini digitali, attraverso l'approccio partecipativo alla rete, costruiscono un complesso di relazioni bidirezionali che hanno determinato il passaggio dalla rete dei contenuti alla rete delle relazioni.

Se fino agli anni Novanta si accedeva a Internet per avere informazioni cercandole direttamente nel sito istituzionale, dagli anni Duemila gli utenti del web hanno cominciato a utilizzare i motori di ricerca, che fungevano da veri e propri intermediari tra i cittadini e le informazioni pubblicate nei siti della PA.

La vera rivoluzione avvenuta a partire dalla seconda metà del primo decennio degli anni Duemila è stata quella di consentire agli utenti del web di avere un contatto diretto con il soggetto detentore delle informazioni: ciò è stato possibile grazie all'avvento dei social network, il cui utilizzo è diventato la principale modalità di ricerca delle informazioni, anche pubbliche.

In questo scenario, in cui la condivisione di informazioni sui social network può generare anche la diffusione di fake news[19], la PA – pur non avendo uno specifico obbligo di presenza sui social[20] – ha più di un motivo per sfruttare tale canale per raggiungere gli obbiettivi di cui si è parlato al par. 1.

Sul punto si riporta la tabella 1 contenuta nel *Vademecum "Pubblica Amministrazione e social media"* che ben riassume come il raggiungimento degli obbiettivi istituzionali possa essere agevolmente raggiunto attraverso le piattaforme.

L'obbiettivo dell'amministrazione non può essere soltanto quello di rispondere pedissequamente alla legge che obbliga alla pubblicazione di alcune informazioni, ma anche quello di assicurarsi che le informazioni pubblicate raggiungano effettivamente i cittadini: in questo senso i social network sono uno strumento di diffusione di grande importanza, in particolare se si tiene in debito conto che «sul sito web dell'Amministrazione il cittadino deve recarsi volontariamente e, per farlo, deve essere spinto dal bisogno di cercare qualcosa. Nei social network il cittadino è presente quasi tutto il giorno, per cui è proprio lì che il bisogno va creato e comunicato»[21].

Proprio sulla scorta della natura ontologicamente partecipativa delle piattaforme social, esse paiono coerenti con la previsione di cui all'art. 7, comma 3 del CAD, il quale prescrive alle amministrazioni di consentire agli utenti di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso all'utente al fine di verificare la qualità del servizio offerto. La possibilità offerta dai social di dialogare senza formalità con l'amministrazione è certamente adatta a raccogliere le impressioni degli utilizzatori e le segnalazioni di malfunzionamento.

In sintesi i social possono rappresentare uno strumento significativo in cui i princìpi di trasparenza, partecipazione ed efficacia della pubblica amministrazione enunciati dalle norme di carattere programmatico possono trovare effettiva attuazione[22], nella misura in cui consentono un dialogo

19. In relazione alle misure tese a limitare la diffusione delle fake news e, più in generale, alle norme di contrasto all'illegalità sul web anche con specifico riferimento alle piattaforme social, si rimanda a quanto già brevemente osservato in ordine ai contenuto del *Digital Service Act* alla nota 15.
20. Pur costituendo una libera scelta della pubblica amministrazione, l'utilizzo dei social media pare incentivato e trovare fondamento normativo nella circolare del Ministero per la Pubblica Amministrazione n. 2/2017 di "Attuazione delle norme sull'accesso civico generalizzato" in cui 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) oltre che in tutta una serie di norme del CAD, in particolare l'art. 2, comma 1 il quale dispone 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».
21. FormezPA 2009.
22. Rossa 2020, p. 208.

più immediato e diretto con la collettività realizzando, al contempo, quel modello di *open government*[23] auspicato dall'ordinamento Ue.

In questo senso si può affermare che, in un'ottica giuspubblicistica, le piattaforme forniscono un rilevante contributo all'effettiva attuazione dei diritti dei cittadini i quali, attraverso l'utilizzo di tale modalità di comunicazione con la PA, riescono ad esercitare in maniera più compiuta rispetto al passato i diritti consacrati nella nostra Carta

	Per l'Amministrazione	Per il cittadino
Efficacia	La presenza nei social network consente di raggiungere il cittadino con maggiore efficacia	La presenza dell'Amministrazione nei social network consente al cittadino di essere informato sulle azioni e sui servizi della PA
Costo	L'ottimizzazione del costo/contatto consente di conseguire maggiori risultati a parità di spesa	L'ottimizzazione del costo/contatto consente di usufruire di un servizio più ampio
Monitoraggio	I social network consentono di monitorare le opinioni dei cittadini sui temi affrontati dall'Amministrazione	L'attenzione della PA verso i temi di interesse per il cittadino si traduce in una maggiore capacità da parte della stessa di cogliere le istanze reali della società
Ascolto, dialogo, fiducia	I social network consentono di sviluppare un dialogo con i cittadini e, attraverso esso, sviluppare un rapporto di fiducia	La disponibilità al dialogo dell'Amministrazione si traduce in una maggiore fluidità nei rapporti
Trasparenza	I social network consentono di sviluppare il concetto di trasparenza da obbligo normativo a strumento di partecipazione	La trasparenza della PA, favorita dal dialogo indotto dai social network, consente uno sviluppo più ampio del sistema dei servizi. La disponibilità di dati pubblici consente al cittadino un maggior livello di consapevolezza e alle aziende di trasformare tali dati in uno strumento di sviluppo
Collaborazione	I social network consentono di attivare meccanismi di collaborazione tra Amministrazione e cittadini, stimolando la cittadinanza attiva e la partecipazione	Lo sviluppo di un rapporto di collaborazione aumenta il livello di consapevolezza

Tabella 1 — Sintesi delle opportunità del social networking per l'amministrazione e per i cittadini (fonte: *Vademecum "Pubblica Amministrazione e social media"*, FormezPA, 2009)

23. Per una trattazione approfondita del tema si veda Faini 2017, p. 324 in cui l'autrice osserva che «nel modello di open government si attualizzano i principi di trasparenza e partecipazione ai tempi del web 2.0, dei social media e delle applicazioni on line, strumenti capaci di abilitare un nuovo modo di condividere i dati e le informazioni, che diventano utilizzabili, aggregabili, sviluppabili da cittadini e imprese. Per valorizzare l'ingresso di queste dimensioni nella realtà delle istituzioni si parla anche di "pubblica amministrazione 2.0". Lo sviluppo dell'amministrazione digitale in questa direzione deriva dalla necessità che le amministrazioni pubbliche siano capaci di parlare lo stesso linguaggio della comunità, alla luce del fatto che trovano la propria ragion d'essere nel realizzare il benessere della collettività: devono quindi comprenderne le esigenze, riuscire a interagire con le modalità relazionali più idonee, cercare di realizzarne la soddisfazione nello svolgimento delle funzioni e nell'erogazione dei servizi. Si tratta pertanto di impiegare i nuovi strumenti nelle politiche e nelle azioni pubbliche, per mezzo di un nuovo approccio caratterizzato dalla condivisione e dalla collaborazione delle istituzioni con altre istituzioni, cittadini, associazioni e imprese».

costituzionale e nel Trattato sull'Unione europea[24], in particolare il diritto alla compartecipazione alla gestione della cosa pubblica e di cittadinanza attiva, intesa come l'opportunità di influenzare le decisioni in modo da contribuire alla costruzione di una società migliore.

Ovviamente la presenza sui principali social network non può essere considerata sostitutiva del sito istituzionale dell'Amministrazione per due ordini di motivi: il primo è che il sito internet è espressamente individuato come canale ufficiale (e obbligatorio) da specifiche norme di legge[25]; il secondo è che l'ente deve garantire la comunicazione e il dialogo anche agli individui che non intendano utilizzare i servizi social.

2. Il contratto di fornitura di social network

Nonostante alcune iniziali resistenze di parte della dottrina[26], è oramai acquisito che l'iscrizione di una persona ad un social network, mediante la registrazione e la creazione di un profilo personale, determina l'insorgenza in capo ai soggetti coinvolti di obblighi e diritti: in altre parole la creazione di un account social costituisce la conclusione di un contratto[27].

Di contro, rimane ancora oggetto di discussione quali siano l'effettiva natura del contratto di social network e la qualificazione giuridica del servizio offerto. Alcuni autori ritengono si tratti di un servizio di accesso a contenuti, altri che si tratti di un servizio assimilabile all'hosting, altri ancora ritengono che si tratti di un vero e proprio servizio di comunicazione. A riguardo si ritiene che l'oggetto del contratto in esame consista in un «servizio di comunicazione interattiva online arricchito di servizi accessori, anche editoriali»[28] o, in termini ancor più generali, nella «fornitura di servizio informatico che si accompagna a determinate inserzioni pubblicitarie»[29].

Per cercare di identificare la disciplina applicabile non rimane che far riferimento alle condizioni d'uso (*terms and conditions*) che sono, ovviamente, predisposte unilateralmente dalla piattaforma e alle quali non è possibile sottrarsi, non essendo prevista alcuna possibilità di contrattazione.

In realtà, anche l'analisi delle condizioni generali di servizio non consente di ricondurre il contratto di social network ad una delle categorie tradizionali ovvero ai tipi noti, e questo per l'impossibilità di far ricorso agli schemi conosciuti dal nostro ordinamento, compresi quelli di solito utilizzati per i contratti aventi ad oggetto la prestazione di servizi: il rapporto tra gestore e utente è infatti caratterizzato dall'interazione tra una indefinita serie di contratti bilaterali conclusi tra la piattaforma stessa e gli altri utenti, che ne determina e ne caratterizza la funzione sociale.

24. L'art. 11 del Trattato sull'Unione europea prevede, ai primi due commi che «1. Le istituzioni danno ai cittadini e alle associazioni rappresentative, attraverso gli opportuni canali, la possibilità di far conoscere e di scambiare pubblicamente le loro opinioni in tutti i settori di azione dell'Unione. 2. Le istituzioni mantengono un dialogo aperto, trasparente e regolare con le associazioni rappresentative e la società civile.» In attuazione di tale norma è stato definito il concetto di "cittadinanza attiva" che significa, in primo luogo, coinvolgimento attivo dei cittadini come partecipazione alla vita delle loro comunità, e quindi alla democrazia, in termini di attività e processo decisionale.
25. Il d.lgs. 82/2005 (CAD) ha trasformato, nel corso degli anni, il sito istituzionale in un vero e proprio front office dell'Amministrazione e un insostituibile strumento di trasparenza.
26. Per una panoramica delle criticità legate alla mancata previsione di obblighi in capo alle parti si veda Astone 2011, p. 108 ss., ove l'autore rileva l'assenza dell'obbligo di pagamento da parte dell'utente e la mancanza di un obbligo di fornire la prestazione da parte della piattaforma.
27. Numerose pronunce dell'AGCOM hanno più volte ribadito la natura contrattuale del rapporto che discende alla creazione di un account social; in particolare si segnala il provvedimento n. 27432 adottato in data 29 novembre 2018, il cui contenuto è stato confermato in sede giurisdizionale da Cons. di Stato 29 marzo 2021, n. 2631 chiamato a decidere sull'impugnazione avverso la sentenza del TAR Lazio che aveva parzialmente accolto l'impugnazione proposta da Facebook avverso la sanzione dell'AGCOM.
28. È questa l'opinione di Zunarelli-Alvisi 2020.
29. Astone 2011, p. 107.

I contratti di social network, considerati unicamente nella dimensione bilaterale tra gestore e singolo utente, avrebbero la singolarità di non avere né causa di scambio, né causa di liberalità, né causa associativa[30], in quanto, analogamente ai contratti di rete[31], paiono svolgere una funzione pratica apprezzabile unicamente qualora si trovino inseriti in un contesto di altre relazioni bilaterali della medesima natura[32].

Del pari anche l'utilizzo della figura del contratto atipico non pare essere di grande aiuto per l'interprete, sia per la difficoltà di ricondurre la struttura del contatto di social network a un tipo conosciuto, sia per la scarsa utilità che ne deriverebbe, posto che le regole dei singoli tipi sono sovente dirette alla soluzione dei conflitti che possono insorgere nella dinamica di uno scambio bilaterale mentre, si è già detto, come il rapporto si riveli multilaterale.

Nonostante il tenore letterale delle condizioni d'uso dei social network, tutti i commentatori della disciplina di questo specifico aspetto del rapporto contrattuale tra utente e piattaforma sono unanimemente certi della natura onerosa del contratto e ciò in contrasto con l'asserita gratuità dichiarata dai gestori delle piattaforme social[33]. Sono ormai numerose le pronunce con cui le autorità giudiziarie europee hanno dichiarato che l'onerosità del contratto di social network è costituita dalla possibilità che il gestore della piattaforma utilizzi i dati personali (in particolare quelli di navigazione) dell'utente il quale, pertanto, ha solamente l'impressione di utilizzare un servizio gratuitamente, mentre in realtà sta "pagando" con le proprie informazioni.

In effetti la valutazione degli interessi in gioco e della concreta operazione economica posta in essere induce a riconoscere che l'accordo tra il social network e l'utente prospetta una regolamentazione mediante la quale l'utente, al fine di ottenere l'accesso alla piattaforma, dispone del diritto alla privacy ed al controllo dei dati personali, consentendo al social network di «raccogliere, usare e condividere i suoi dati». Già i primi commentatori avevano rilevato che «tra il gestore del sito del social network e l'utente è concluso un accordo di scambio non più soltanto "di fatto" o economico, bensì un contratto di scambio "giuridico"»[34] da cui discenderebbero obblighi in capo al gestore della piattaforma, il quale dovrebbe garantire la fornitura del servizio e assicurare il corretto funzionamento della piattaforma, dal momento che queste prestazioni costituiscono il corrispettivo dell'autorizzazione concessa dall'utente.

Sul punto si osserva sin d'ora (ma il tema verrà ripreso in seguito) che tutti i diritti collegati ai contenuti pubblicati dagli utenti diventano di "proprietà" del social network, per espressa previsione del contratto accettato al momento dell'apertura del profilo personale.

Ma trattandosi di un vero e proprio contratto, prima di passare all'analisi delle specifiche previsioni contenute nelle condizioni d'uso, è necessario interrogarsi su chi sia il soggetto legittimato a concludere il contratto con la piattaforma qualora s'intenda aprire un profilo di un ente pubblico.

3. La policy di Facebook

3.1. Account necessariamente legato ad una persona fisica

Con particolare riferimento a Facebook (ma anche ad Instagram, facente capo allo stesso gruppo guidato da Meta Platforms Inc., società di diritto statunitense), la prima criticità che si pone è quella relativa all'impossibilità, per un ente, di aprire direttamente ed autonomamente una pagina pubblica: la piattaforma, infatti, consente esclusivamente la

30. La migliore dottrina civilistica riconduce tradizionalmente le funzioni del contratto a tre: scambio, liberalità e associazione (Rescigno 2000, p. 271).
31. Ci si riferisce al franchising o al *chain of contract*.
32. Astone 2011, p. 112.
33. Anche chi non inquadra il contratto di social network tra i contratti con corrispettivo, esclude comunque che possa trattarsi di un contratto liberale, in quanto «non caratterizzato dall'intento di arricchire l'altra parte prestando gratuitamente un servizio» (Astone 2011, p. 109).
34. È questa la opinione di Perlingieri 2018.

creazione di profili personali, legati cioè all'identità di una persona fisica ed impedisce la creazione di profili legati a persone giuridiche[35].

Pertanto, qualora un dipendente pubblico aprisse un account per conto dell'ente di appartenenza e utilizzasse il diario per le comunicazioni istituzionali dell'ente, ci sarebbe il fondato rischio che il fornitore del servizio sospenda le pubblicazioni poiché in violazione delle condizioni d'uso[36].

D'altronde, l'unica possibilità per un ente pubblico di utilizzare Facebook, conformemente alle condizioni d'uso attualmente vigenti, è quella di far aprire una pagina pubblica da un profilo personale di un dipendente.

Facebook consente, infatti, al titolare di un account personale di creare una pagina pubblica riferita ad una persona giuridica (pubblica o privata) ma questa modalità genera una serie di criticità legate alla rappresentanza dell'ente e all'imputazione a quest'ultimo dei contenuti pubblicati sulla pagina pubblica, oltre che in ordine alla ripartizione delle responsabilità (civili, penali e amministrative) che potrebbero derivare dall'utilizzo del profilo pubblico.

Pertanto nel caso di Facebook, diversamente da quanto previsto da altri social network (ad es. Twitter[37]), la pubblica amministrazione non è parte del contratto[38] ma rimane terza beneficiaria del contratto perfezionato dal dipendente, il quale per poter assumere il ruolo di intermediario tra il proprio ente e la piattaforma dovrà essere autorizzato in forza di apposito mandato (sul punto di veda *infra* par. 5.1).

A riguardo si è fatto notare che negli *standard della community* di Facebook è previsto che «Le pagine […] non devono fare le veci o rappresentare in modo falso […] un ente […]». Tale previsione viene considerata la fonte contrattuale che rende legittima l'apertura di una pagina di una pubblica amministrazione: essa può infatti costituire il consenso della piattaforma all'apertura di una pagina di un ente pubblico da parte di un dipendente, qualora questi abbia ricevuto uno specifico mandato[39].

3.2. Il problema dell'eredità digitale

In caso di morte del soggetto titolare di un account le condizioni d'uso di Facebook (che, si ricorda, sono sempre predisposte unilateralmente dalla piattaforma) prevedono diversi scenari che possono essere preventivamente gestiti dal titolare. È infatti possibile prevedere che il profilo privato rimanga visibile dopo la morte dell'interessato unicamente a fini commemorativi e lo stesso possa essere gestito da una persona appositamente individuata come "contatto erede" [40].

Il "contatto erede" potrebbe tuttavia non coincidere con il successore *mortis causa* il quale sarebbe l'unico, secondo le norme dell'ordinamento italiano, a poter vantare l'effettiva titolarità dei diritti di proprietà intellettuali (patrimoniali e morali) sui contenuti pubblicati dal *de cuius* sul profilo privato e dei diritti eventualmente ad esso collegati, come ad esempio i privilegi derivanti dall'essere amministratore di una pagina pubblica.

Tale disciplina potrebbe creare non pochi problemi all'ente la cui pagina pubblica sia stata creata

35. La clausola 3.1 delle condizioni d'uso di Facebook, recita «l'utente è tenuto a: usare lo stesso nome di cui si serve nella vita reale; fornire informazioni personali accurate; creare un solo account (il proprio) e usare il proprio diario per scopi personali».
36. La clausola 4.2 delle condizioni d'uso di Facebook attribuisce alla piattaforma il potere di «sospendere o disabilitare in modo permanente l'accesso dell'utente al suo account» nell'ipotesi in cui Facebook «stabilisca che l'utente abbia violato chiaramente, seriamente o reiteratamente le proprie condizioni normative».
37. Twitter consente infatti alle persone giuridiche di aprire direttamente un account a loro nome senza utilizzare un profilo privato.
38. Questa circostanza comporta la esclusione dell'applicabilità al caso di specie delle disposizioni del d.lgs. 31 marzo 2023, n. 36 (nuovo Codice dei contratti pubblici).
39. Sul punto si osserva che, ai sensi delle condizioni generali di servizio di Facebook, non sarebbe neppure possibile creare un profilo di una persona inesistente o immaginaria, così come è vietato fornire informazioni personali false o creare un account per un'altra persona senza autorizzazione, pena la disattivazione del servizio.
40. Il "contatto erede" non potrà comunque leggere i messaggi privati né modificare i contenuti pubblicati dal *de cuius* ed accederà al profilo commemorativo con poteri gestori ridotti, cfr. Marino 2018, p. 1.

da un dipendente in seguito deceduto, perché ci si potrebbe trovare nell'impossibilità di accedere ai contenuti della pagina istituzionale. A riguardo sarebbe opportuno disciplinare in maniera chiara che la titolarità dei contenuti pubblicati sul profilo pubblico appartiene all'ente ed eseguire, prudenzialmente, dei backup periodici da conservare in locale nella disponibilità dell'ente.

Le medesime criticità si verificherebbero anche nel caso di dipendente trasferito, promosso o adibito ad altro incarico, così come nel caso di pensionamento o, comunque, di cessazione del rapporto di lavoro. In tutti questi casi, le difficoltà possono essere superate mediante l'adozione di provvedimenti che istituiscano una specie di "catena" di soggetti dotati degli opportuni privilegi e gravati dai conseguenti obblighi, così da scongiurare l'eventualità che, in caso di scomparsa o impossibilità ad accedere alla rete dell'unico soggetto responsabile, si determini l'interruzione del servizio o la perdita di dati.

3.3. Legge applicabile e foro competente

Le modalità di apertura di una pagina pubblica fin qui descritte hanno dei risvolti di non poco conto anche in ordine alla tutela dei diritti dei soggetti coinvolti. Infatti la qualifica soggettiva della parte che effettivamente entra in contatto con la piattaforma determina conseguenze in particolare sulla legge applicabile al rapporto contrattuale e al foro competente a risolvere eventuali controversie.

Quanto alle questioni che vedono coinvolto il soggetto titolare del profilo privato sono possibili tre scenari differenti.

Il primo è quello di un soggetto persona fisica che utilizzi la piattaforma per scopi estranei all'attività professionale: in questo caso troverà applicazione la normativa a tutela dei consumatori e pertanto, come confermato anche dalle condizioni d'uso di Facebook, sarà applicabile la legge e la giurisdizione dello Stato membro dell'Unione europea in cui risiede la persona fisica consumatore.

Il secondo è quello di un soggetto persona fisica che utilizzi la piattaforma per scopi professionali, nel qual caso, secondo la previsione delle condizioni d'uso di Facebook, sarà applicabile la legge e la giurisdizione irlandese, quale Stato in cui Facebook (prima) e Meta Platforms Inc. (poi) hanno stabilito la sede nell'Unione europea.

Il terzo è quello dell'utilizzo dei servizi offerti dalla piattaforma per scopi aziendali: in questo caso troveranno applicazione le norme contenute nelle *Condizioni commerciali di Facebook*, le quali – integrando il contenuto delle condizioni generali d'uso – prevedono il rinvio alla legge dello Stato della California e, al fine della risoluzione delle eventuali controversie, rinviano ad un arbitrato disciplinato dal *Federal Arbitration Act* e, in via residuale, alla Corte distrettuale USA per la California settentrionale o ad un tribunale situato nella contea di San Mateo, ubicata nella San Francisco Bay Area.

Per quanto d'interesse per il presente elaborato e con specifico riferimento alla pagina pubblica di una persona giuridica (sia essa di diritto privato o di diritto pubblico) si ritiene che la natura del soggetto coinvolto nonché l'attività svolta sulla pagina pubblica consenta di escludere l'applicazione della normativa a tutela dei consumatori, così come anche la qualifica di professionista del dipendente che opera in nome e per conto dell'ente.

Ergo non rimane che la terza ipotesi, anche alla luce del fatto che la PA, essendo sottratta alla disciplina a tutela dei consumatori, non potrà validamente contestare la vessatorietà della previsione di una giurisdizione straniera, posto che l'attività svolta in nome e per conto dell'ente dal dipendente ricade – senza dubbio – nel concetto di uso aziendale e non personale.

La conseguenza è che il rapporto tra l'ente pubblico e Facebook non può che essere disciplinato dalla legge dello Stato della California e le eventuali controversie sull'utilizzo della pagina pubblica dovranno essere risolte da un arbitrato disciplinato dal *Federal Arbitration Act* e, in via residuale, da uno degli organismi poc'anzi ricordati ed aventi sede in California.

4. Imputazione soggettiva delle comunicazioni e delle attività svolte sulla pagina istituzionale

Si è già detto al par. 3 che, nel caso di Facebook (e di tutti quei social che non consentono la creazione di un profilo pubblico direttamente da parte dell'ente) le parti del contratto di social network sono il soggetto titolare del profilo privato e la piattaforma, mentre l'ente risulta terzo beneficiario.

Da ciò discende che tutte le azioni contrattuali esercitabili (adempimento, inadempimento, risoluzione, risarcitoria) spettano al titolare dell'account

privato del dipendente, salvo – ovviamente – quelle esercitabili direttamente dal terzo beneficiario a tutela dei diritti che lo stesso mutua dal contratto di fornitura di servizi perfezionato dal dipendente. Ci si riferisce, ad esempio, al caso di mancata pubblicazione nella piattaforma di un contenuto perché ritenuto in violazione degli *standard della community* e come tale filtrato automaticamente da un software (senza l'intervento umano), mentre – di contro – la pubblicazione di quel contenuto viene considerata dall'ente come necessaria per raggiungere gli obiettivi di comunicazione fissati dal piano di comunicazione[41].

In dottrina è stato anche evidenziato che, nel caso in cui il titolare di un profilo personale abbia aperto un profilo pubblico senza autorizzazione e agisse come *falsus procurator* ovvero eccedendo il mandato ricevuto, da un lato violerebbe le condizioni d'uso della piattaforma, la quale potrebbe sospendere il relativo servizio; dall'altro l'ente falsamente rappresentato avrebbe l'onere di intervenire presso la piattaforma per rimuovere i contenuti e la pagina creata spendendo il nome dell'amministrazione senza autorizzazione, al fine di evitare che in applicazione dell'istituto della rappresentanza apparente i contenuti illegittimamente pubblicati possano essere imputati soggettivamente all'ente: in definitiva una sorta di onere di disconoscimento in capo alla PA falsamente rappresentata.

4.1. Imputazione all'ente della responsabilità contrattuale per fatto del dipendente

Cambiando la prospettiva da cui si osserva tale configurazione contrattuale, è necessario chiedersi se la piattaforma possa imputare direttamente alla PA la responsabilità derivante dalla violazione delle condizioni d'uso effettuata dal dipendente in occasione della pubblicazione di contenuti in nome e per conto dell'ente.

Limitando l'analisi al solo Facebook – escludendo pertanto dall'ipotesi in esame Twitter[42] – la risposta pare essere condizionata dall'esistenza di un mandato dell'ente in favore del dipendente poiché, ovviamente, se quest'ultimo vìola le condizioni d'uso in esecuzione del mandato ricevuto sarà responsabile a titolo d'inadempimento contrattuale nei confronti del fornitore del servizio in solido con l'ente mandante il quale risponderà, a titolo extracontrattuale *ex* art. 2043 c.c., per aver indotto il proprio dipendente a violare le condizioni d'uso.

Diversamente, qualora la violazione delle condizioni d'uso di Facebook avvenga contravvenendo alle istruzioni impartite dalla PA mandante, il dipendente risponderebbe personalmente a titolo contrattuale ma non troverebbe applicazione l'art. 2043 c.c., non potendo configurarsi alcuna responsabilità extracontrattuale (diretta) dell'ente.

Rimane però un'ulteriore ipotesi di responsabilità indiretta dell'ente, il quale potrebbe essere chiamato a rispondere ai sensi dell'art. 2049 c.c.[43], per il fatto illecito del proprio dipendente, nell'ipotesi in cui il comportamento di quest'ultimo abbia causato un danno di natura aquiliana alla piattaforma.

4.2. Imputazione all'ente della responsabilità extracontrattuale per fatto del dipendente

Il tema della riferibilità alla PA delle condotte illecite del proprio dipendente è stato oggetto di un animato confronto tra dottrina e giurisprudenza e la stessa Suprema Corte di Cassazione è giunta a volte ad approdi contrastanti: un primo orientamento (restrittivo) circoscriveva la responsabilità dell'ente ad ipotesi limitate a condotte abnormi del dipendente; un secondo orientamento (estensivo) espandeva la responsabilità anche ad ipotesi in cui la condotta del dipendente risultava anche solo labilmente collegata al datore di lavoro pubblico.

Senza indagare a fondo le ragioni dei contrasti interpretativi, essendo fuori dell'oggetto del presente lavoro, è sufficiente ricordare che la giurisprudenza civile, ravvisando il fondamento della

41. Il caso è meno infrequente di quanto possa sembrare, specialmente in occasione di pubblicazione di immagini per le quali Facebook prevede un esame volto a verificare a presenza di nudità e, spesso, il filtro non accetta la pubblicazione di riproduzioni di opere d'arte solamente poiché individuate dal software come "nudo volgare" o come "contenuto forte" non adatto al tutto il pubblico.
42. Del quale si è già riferito di come consenta l'apertura di un profilo pubblico direttamente dall'ente e, pertanto, non v'è dubbio che la violazione dei termini d'uso determini responsabilità contrattuale in capo all'ente stesso.
43. Art. 2049 c.c. «I padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti».

responsabilità dello Stato e degli enti pubblici per il fatto illecito dei propri dipendenti nell'art. 28 della Costituzione (e il conseguente principio di immedesimazione organica del dipendente con l'ente) riteneva che la PA dovesse rispondere dell'illecito del dipendente solamente qualora l'attività dannosa fosse direttamente collegata (o collegabile) allo Stato o all'ente pubblico, cioè tendesse al conseguimento dei fini istituzionali nell'ambito delle attribuzioni dell'ufficio o dei compiti del dipendente[44]. In tale maniera risultava esclusa la responsabilità dell'ente ogni qualvolta il dipendente avesse avuto fini esclusivamente privati ed egoistici e, a maggior ragione, quando la condotta del dipendente fosse contraria con i fini istituzionali dell'ente.

A tale interpretazione si contrapponeva quella della giurisprudenza penale, la quale invece riconosceva la responsabilità civile (conseguente da reato) in capo all'amministrazione anche nell'ipotesi di condotte dei pubblici dipendenti volte a perseguire interessi personali, qualora tali condotte fossero poste in essere sfruttando la posizione "privilegiata" conseguente al proprio ruolo istituzionale ed ogni qualvolta ciò costituisse un «non imprevedibile sviluppo dello scorretto esercizio di tali funzioni pubbliche»[45].

A risolvere tale contrasto intervenivano le Sezioni Unite della Suprema Corte di Cassazione le quali, con sentenza n. 13246 del 16 maggio 2019, rilevando un «ingiustificato privilegio della Stato o dell'ente pubblico» nell'interpretazione restrittiva, optavano per ricondurre la responsabilità dell'ente pubblico da fatto illecito del proprio dipendente sullo stesso piano di quella di ogni privato preponente, in applicazione dei principi desunti dall'art. 2049 c.c. Le Sezioni Unite finivano, quindi, per riconoscere la responsabilità del datore di lavoro anche nel caso di condotta del dipendente deviante o contraria rispetto ai fini istituzionali purché *i*) si tratti di condotte caratterizzate da un legame di causalità necessaria[46] e *ii*) si tratti di condotte oggettivamente raffigurabili o prevedibili.

Calando tale principio sul tema dell'utilizzo delle piattaforme social network da parte delle PA, a fronte della condotta del dipendente che, accedendo con le proprie credenziali alla pagina pubblica dell'ente in quanto amministratore, dovesse pubblicare contenuti diffamatori oppure dovesse caricare contenuti in violazione della normativa a tutela del diritto d'autore ovvero di quella in materia di dati personali[47], si potrebbe sostenere la responsabilità (indiretta) del datore di lavoro pubblico *ex* art. 2049 c.c.

5. Rapporto trilaterale tra piattaforma, dipendente ed ente

Della non gratuità del contratto di social network si è già detto al par. 2 ma il tema, soprattutto nella prospettiva di un ente pubblico, merita di essere approfondito poiché l'effettiva onerosità dello stesso impone l'individuazione del soggetto che, nella sostanza, corrisponde la controprestazione.

Come correttamente osservato in dottrina[48] «il contratto tra social network e utente deve essere ricondotto nell'alveo dei contratti di scambio poiché la disposizione della privacy e dei dati personali è in funzione dell'utilizzo della piattaforma sì che in virtù del sinallagma l'utente in tanto ha diritto di utilizzare la piattaforma – e il social è obbligato a consentirne l'utilizzo – in quanto il social può raccogliere e sfruttare i dati personali».

Inoltre deve essere tenuto in considerazione che tale contratto è funzionalmente collegato con i contratti di pubblicità conclusi dalla piattaforma con gli inserzionisti[49], in virtù dei quali Facebook riceve il pagamento di somme di denaro per consentire alle aziende commerciali di pubblicare i propri annunci pubblicitari in maniera selettiva, cioè facendo in modo che siano visibili solamente a certi utenti (e non ad altri) individuati come

44. Cfr. Cass. civ. 12 agosto 2000, n. 10803; Cass. civ. 30 gennaio 2008, n. 2089, Cass. civ. 17 settembre 1997, n. 9260.
45. Cfr. Cass. pen. 31 marzo 2015, n. 13779.
46. Nel senso che la condotta è stata resa possibile proprio dai poteri conferiti dall'ente al dipendente.
47. Per un elenco, per quanto non esaustivo, della normativa di riferimento si veda il par. 1.
48. Perlingieri 2014, p. 90 ss.
49. Profilo su cui ci si è già soffermati in precedenza e che è stato sin da subito considerato come elemento che consentisse di escludere la gratuità del servizio, cfr. Astone 2011, p. 114 ove l'autore parla di «gratuità interessata» per descrivere l'utilità economica sottesa al negozio giuridico concluso tra piattaforma e utente.

maggiormente interessanti in quanto precedentemente "profilati"[50] dalla piattaforma stessa.

Sul punto non paiono esserci dubbi in quanto è lo stesso Facebook che lo palesa nelle condizioni d'uso[51] dalla cui lettura emerge un quadro sufficientemente chiaro: Facebook autorizza l'utente persona fisica ad utilizzare la sua piattaforma e godere dei relativi contenuti; di contro l'utente persona fisica concede a Facebook licenza di utilizzo di tutti i contenuti che carica online (ivi compresi i diritti d'autore sui contenuti originali) nonché, e soprattutto, dei propri dati personali ricavabili dall'utilizzo della piattaforma stessa. Si tratta dei cosiddetti dati di navigazione, dall'analisi dei quali è possibile ricavare informazioni utili per riuscire a "profilare" le persone[52] ai fini di marketing.

In questo senso si è espressa l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) la quale, con provvedimento del 29 novembre 2018 n. 27432, ha per la prima volta condannato Facebook per pratiche commerciali ingannevoli per aver pubblicizzato l'asserita gratuità del servizio mentre, di contro, dall'attenta lettura delle condizioni d'uso emerge un "corrispettivo" in dati personali pagato dall'utente, inducendolo così «ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (registrazione al social network e permanenza nel medesimo)».

Anche il TAR del Lazio, con pronuncia del 10 gennaio 2020 n. 260, pur accogliendo parzialmente l'opposizione proposta da Facebook, ha confermato tale valutazione, ritenendo che «il fenomeno della patrimonializzazione del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto della scambio di prestazioni che è sotteso all'adesione ad un contratto per la fruizione di un servizio quale è quello di utilizzo di un social network».[53]

Pertanto, nel caso di apertura di una pagina pubblica di un ente tramite un profilo personale

50. Per un esame dell'attività di profilazione sui social si veda European Data Protection Board 2021.
51. Paragrafo 2 delle condizioni d'uso Facebook «Come vengono finanziati i servizi di Facebook» si legge «Anziché pagare per l'uso di Facebook e degli altri prodotti e servizi offerti, utilizzando i Prodotti di Facebook coperti dalle presenti condizioni, l'utente accetta che Facebook possa mostrare inserzioni la cui promozione all'interno e all'esterno dei prodotti delle aziende di Facebook avviene dietro pagamento da parte di aziende e organizzazioni. Facebook usa i dati personali dell'utente (ad esempio informazioni su attività ed interessi) per mostrargli le inserzioni più pertinenti». Al paragrafo 3.3.1 è poi previsto che «l'utente deve concedere [a Facebook] determinate autorizzazioni […] all'uso dei contenuti creati e condivisi dall'utente […] nello specifico, quando l'utente condivide, pubblica o carica un contenuto protetto da diritti di proprietà intellettuale in relazione o in connessione con i Prodotti di Facebook, concede una licenza non esclusiva, trasferibile, sub-licenziabile, non soggetta a royalty e valida in tutto il mondo per la trasmissione, l'uso, la distribuzione, la modifica, l'esecuzione, la copia, la pubblica esecuzione o la visualizzazione, la traduzione e la creazione di opere derivate dei propri contenuti […]. Ciò implica ad esempio che se l'utente condivide una foto su Facebook autorizza Facebook a memorizzarla, copiarla e condividerla con altri soggetti […] quali i fornitori di servizi che supportano il servizio o gli altri Prodotti di Facebook che l'utente usa. La presente licenza cessa di esistere una volta eliminati i contenuti dell'utente dai sistemi di Facebook […] tuttavia potrebbero continuare ad esistere in altri luoghi all'interno dei sistemi Facebook […]». Inoltre, ai sensi del paragrafo 3.3.2 si legge «l'utente autorizza Facebook a usare il proprio nome, l'immagine del profilo e le informazioni relative alle azioni intraprese su Facebook in relazione o in connessione a inserzioni, offerte e altri contenuti sponsorizzati che Facebook mostra all'interno dei suoi Prodotti, senza alcuna remunerazione a suo vantaggio. Ad esempio Facebook potrebbe mostrare agli amici dell'utente il suo interesse nei confronti di un evento sponsorizzato o che l'utente ha messo "Mi piace" a una Pagina creata da un brand che ha retribuito Facebook per mostrarne le inserzioni su Facebook».
52. A riguardo si può ragionevolmente ipotizzare che alla base della scelta di Facebook di non concludere alcun contratto direttamente con le persone giuridiche, sia private che pubbliche, ci sia la circostanza che tali soggetti non sono idonei ad essere sfruttati per la raccolta dati ai fini commerciali.
53. Sentenza poi confermata dal Consiglio di Stato (sez. VI, 29 marzo 2021, n. 2631) investito della questione a seguito dell'impugnazione proposta da Facebook e dall'AGCOM avverso detta sentenza del TAR Lazio.

di un dipendente, l'ente in questione beneficerebbe gratuitamente della possibilità di utilizzare la propria pagina istituzionale in quanto il corrispettivo previsto dal contratto di social network graverebbe tutto sul dipendente, il quale mette a disposizione di Facebook tutti i propri dati.

5.1. Necessità di predisporre atti amministrativi con incarico e compenso

Come osservato *supra*, in virtù delle scelte contrattuali effettuate unilateralmente dal prestatore del servizio di social network, la comunicazione istituzionale delle pubbliche amministrazioni finirebbe per essere remunerata con i dati personali del dipendente, con i suoi diritti d'autore sui contenuti caricati sul diario personale oltre che con quelli pubblicati sulla pagina istituzionale.

Tale circostanza lascia prefigurare uno scenario potenzialmente critico per la PA, poiché il dipendente potrebbe imputare al proprio ente un arricchimento senza causa per aver beneficiato di un servizio senza corrispondere la relativa controprestazione che graverebbe, per intero, sul dipendente stesso.

Per tali motivi è necessario che le scelte dell'amministrazione in merito all'apertura e alla gestione degli account social passino attraverso il consueto *iter* amministrativo che caratterizza l'operato della PA. È necessario cioè che l'ente adotti uno specifico provvedimento con il quale l'organo esecutivo dell'ente[54], dato atto della necessità di utilizzare una determinata piattaforma social per adempiere ai doveri di comunicazione imposti dalla legge 7 giugno 2000 n. 150, individui uno o più dipendenti come responsabili di questa specifica attività, i quali dovranno aver previamente prestato il consenso all'assunzione di tale impegno.

Il consenso del dipendente dovrà riguardare non solo l'assunzione degli incombenti cui sarà gravato in forza del provvedimento datoriale (aggiornare la pagina con i contenuti concordati con l'amministrazione, verificare il corretto funzionamento dell'account, fungere da moderatore delle discussioni quando ciò è consentito etc.) ma dovrà comprendere anche l'accettazione dell'utilizzo del proprio account personale per la creazione della pagina pubblica. Il mandato conferito dal datore di lavoro infatti dovrà prevedere l'impegno (gravante sul dipendente) di creare, utilizzare e mantenere attiva l'utenza personale per consentire all'ente di poter usufruire dei servizi di social network per la pagina istituzionale.

Stante la multidisciplinarità che caratterizza tale mansione, il dipendente dovrà anche ricevere un'adeguata formazione, a cura del datore di lavoro, con particolare riguardo al funzionamento delle reti telematiche e alla sicurezza informatica. Occuparsi della comunicazione tramite social richiede infatti differenti competenze sia di natura informatica che giuridica che devono essere necessariamente patrimonio culturale dell'operatore che agisce, tramite le reti, in nome e per conto di un'amministrazione pubblica.

Ovviamente al dipendente andrà riconosciuta una indennità per lo svolgimento di tale servizio per due ordini di motivi: il primo è legato alla remunerazione della disponibilità del dipendente a pagare il corrispettivo del contratto di social network con i propri dati personali, evitando così che il dipendente possa lamentare un arricchimento senza causa dell'ente in suo danno[55].

Il secondo motivo è più strettamente legato alle norme che regolano il rapporto di lavoro pubblico, in forza delle quali il dipendente deve fornire la prestazione lavorativa secondo le modalità imposte dal datore di lavoro il quale, a sua volta, non può pretendere prestazioni non previste dal contatto collettivo di lavoro senza riconoscere un adeguato compenso.

Pertanto, verificata la presenza di tale attività nella declaratoria del CNNL applicabile alla posizione lavorativa del dipendente, per la remunerazione dell'attività svolta da quest'ultimo in forza dello specifico mandato conferito dall'ente

54. Anche il *Vademecum "Pubblica Amministrazione e social media"* più volte citato suggerisce che la decisione relativa all'iscrizione ad un social venga presa (o quantomeno autorizzata) dal soggetto che, in base all'ordinamento dell'ente, è in grado di impegnarlo verso l'esterno.

55. Una sorta d'indennizzo per le conseguenze che potenzialmente il dipendente potrebbe subire in ragione dell'utilizzo dei suoi dati personali da parte della piattaforma. Si pensi, ad esempio, agli annunci pubblicitari personalizzati e alle note questioni legate all'accettazione dei cookies che si ripercuoteranno direttamente e personalmente sul dipendente.

potrebbe utilizzarsi la quota variabile del fondo risorse decentrate (o di produttività) previsto per i diversi comparti del pubblico impiego[56].

Sul punto si anticipa sin d'ora che la predisposizione di un mandato scritto che contenga indicazioni precise sulle attività che il dipendente deve compiere in nome e per conto dell'amministrazione delegante svolge anche la funzione di garantire la conformità di tale attività alla disciplina a tutela dei dati personali (il tema verrà trattato *infra* al par. 7).

6. La responsabilità disciplinare del dipendente

L'adozione di un provvedimento con cui l'ente individua specificatamente i compiti assegnati al dipendente, indicandone al contempo il compenso, ha effetti positivi sul rapporto di lavoro in termini di chiarezza tra le parti e responsabilizzazione del dipendente: infatti quest'ultimo avrà ben chiaro quali sono i suoi obblighi e i suoi diritti e d'altro canto sarà più facile per il datore di lavoro pretendere il rispetto delle specifiche istruzioni impartite e, in caso di violazioni, effettuare le opportune contestazioni disciplinari.

Inoltre, in applicazione della previsione di cui all'art. 54, comma 1, del d.lgs. 30 marzo 2001, n. 165 (Testo Unico Pubblico Impiego)[57], il Governo ha emanato il Codice di comportamento dei dipendenti della pubblica amministrazione, contenuto nel d.P.R. 16 aprile 2013, n. 62, che costituisce una ulteriore fonte di diritto idonea a fondare responsabilità disciplinare in caso d'inosservanza delle sue prescrizioni. Esso infatti si applica a tutto il personale della pubblica amministrazione (ivi compresi gli enti territoriali), ai soggetti non dipendenti quali collaboratori o consulenti, nonché ai collaboratori a qualsiasi titolo di imprese fornitrici di beni e servizi[58], con l'esclusione del personale "politico" ovvero i funzionari onorari che compongono, per elezione o nomina, gli organi politici di vertice delle amministrazioni[59].

A ciò si aggiunga che l'art. 54, comma 5 del TUPI impone alle singole amministrazioni l'adozione di un proprio Codice di comportamento ad integrazione e specificazione del Codice di comportamento c.d. "generale". Infatti, mentre il Codice di comportamento introdotto dal d.P.R. 62/2013 definisce gli obblighi "minimi" di diligenza, lealtà, imparzialità e buona condotta cui devono attenersi tutti i funzionari pubblici, ogni singolo ente è tenuto ad adottare un atto che contenga la specificazione di tali regole generali e che le traduca in indicazioni chiare e adeguate alle specificità di ciascuna amministrazione.

La responsabilità disciplinare dei dipendenti conseguente all'utilizzo dei social network è stata oggetto di numerose pronunce che hanno affrontato questo tema a partire dalla seconda decade degli anni 2000.

Con riferimento al rapporto di lavoro privato, la giurisprudenza ha riconosciuto la responsabilità disciplinare per violazione del dovere di fedeltà imposto dagli artt. 2104 e 2015 c.c. qualora il dipendente ponga in essere comportamenti suscettibili di danneggiare l'immagine aziendale, ad esempio attraverso la pubblicazione di contenuti osceni, volgari od offensivi sulle principali piattaforme social[60].

Analoga responsabilità è stata individuata con riferimento al rapporto di lavoro pubblico: la Cassazione ha infatti ritenuto legittima la sanzione disciplinare comminata ad un militare per aver recato pregiudizio all'immagine dell'amministrazione mediante la pubblicazione di contenuti fortemente critici nei confronti della propria amministrazione, in contrasto con la normativa speciale prevista dall'ordinamento militare[61].

56. Fondo che per quanto concerne il comparto Regioni-Enti Locali è disciplinato dall'articolo 15 del CCNL 1° aprile 1999.
57. Nella riscrittura operata dalla legge 6 novembre 2012, n. 190.
58. In forza dell'art. 2, comma 2 del Codice di comportamento dei dipendenti della pubblica amministrazione.
59. Per un'analisi delle conseguenze della scelta del legislatore di escludere dal perimetro di applicazione della norma in esame il personale di nomina politica, si veda Carloni 2013, p. 402.
60. Con riferimento al datore di lavoro privato si vedano Cass. pen., sez. I, 16 aprile 2014, n. 16712; Cass. civ., sez. lav., 27 aprile 2018, n. 10280; C. App. Torino 17 luglio 2014, Tribunale di Ivrea 28 gennaio 2015.
61. Cfr. TAR Friuli Venezia Giulia – Trieste, 12 dicembre 2016, n. 562.

A prescindere dall'applicazione della normativa speciale, come nel caso del dipendente militare, si ritiene che l'art. 3, comma 3 del Codice di comportamento possa costituire l'addentellato normativo su cui poter fondare la responsabilità disciplinare di tutti pubblici dipendenti in caso di pubblicazione di contenuti osceni, volgari od offensivi, quantunque nel proprio profilo privato. La norma richiamata prevede infatti che «il dipendente deve evitare situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine della pubblica amministrazione» quale obbligo che specifica il principio generale di diligenza e fedeltà del dipendente.

Di contro non paiono esserci dubbi sulla sussistenza della responsabilità disciplinare del dipendente che, in violazione delle prescrizioni impartite dall'amministrazione, faccia un utilizzo della pagina social dell'ente non conforme ai principi enunciati nel Codice di comportamento[62] e che sia suscettibile di danneggiare l'immagine dell'amministrazione di appartenenza[63].

7. Il problema della conformità al GDPR

Pur non essendo oggetto del presente lavoro, si ritengono necessari alcuni cenni alle criticità legate all'utilizzo dei social network da parte delle pubbliche amministrazioni in ordine al rispetto della normativa a tutela dei dati personali.

Come correttamente osservato da alcuni commentatori[64], l'ente pubblico che utilizza un account social può rivestire allo stesso tempo il ruolo di utilizzatore (*user*) dell'account social – quantunque non tutelato dal GDPR[65] – ma anche quello di titolare (*data controller*) dell'eventuale trattamento dei dati personali: tale ultima evenienza si verificherebbe nel caso in cui tramite la pagina pubblica vengano raccolte, pubblicate, condivise, "taggate", conservate o cancellate informazioni riguardanti una persona fisica identificata o identificabile come interessato (*data subject*).

Il rischio di un siffatto trattamento "involontario" di dati potrebbe essere abbattuto adottando per policy interna le impostazioni che la piattaforma mette a disposizione dell'amministratore della pagina pubblica, il quale può personalizzare – sin dal momento della creazione dell'account – alcune funzioni: ad esempio, è possibile impedire la condivisione da parte degli utenti dei contenuti pubblicati, disattivare la chat di messaggistica istantanea, impedire l'invio di messaggi attraverso applicazioni di terze parti e, soprattutto, impedire che gli utenti possano pubblicare contenuti sulla bacheca della pagina pubblica, ovvero "taggare" altri utenti e caricare foto o video.

Ad ogni modo si ritiene che non sia possibile eliminare totalmente il rischio che, attraverso l'utilizzo della pagina pubblica, si realizzi un trattamento di dati personali, in particolar modo se si considera l'interpretazione estensiva data dalla giurisprudenza dell'esatta portata semantica dell'apposizione in un "mi piace" ad un post. Se, come si è visto al par. 6[66], la semplice apposizione di un "like" equivale ad una manifestazione di pensiero, quantomeno nella forma dell'adesione al contenuto del post in questione, ne deriva che, qualora da tale manifestazione sia possibile ricavare una informazione, questa dovrebbe essere certamente ricondotta nel novero dei dati personali, con conseguente applicazione dell'impianto normativo previsto dal GDPR e l'inevitabile conseguenza di dover considerare l'ente quale titolare del trattamento.

D'altronde il carattere pubblico degli account in questione impedisce che possa trovare applicazione l'*household exemption* prevista dall'art

62. Ciò in forza del combinato disposto dell'art. 54, comma 3 TUPI e dell'art. 3, comma 3 del Codice di comportamento.
63. TAR Lombardia, sez. III, ord. 3 marzo 2016, n 246 ha ritenuto che anche solo «l'aggiunta del commento "mi piace" ad una notizia pubblicata su Facebook può ben comportare un danno all'immagine dell'amministrazione e pertanto assume rilevanza disciplinare», pronuncia relativa ad un caso in cui un dipendente dell'Amministrazione Penitenziaria aveva messo "mi piace" alla notizia di un suicidio di un detenuto.
64. Cfr. Zunarelli-Alvisi 2020, p 41.
65. Il GDPR limita l'applicazione dell'impianto normativo di tutela dei dati personali solamente alle persone fisiche e gli enti pubblici, in quanto persone giuridiche, non possono beneficiarne.
66. Si veda a riguardo quanto riferito alla nota 51.

2.2, lett. c) del GDPR, e ciò anche in ragione delle finalità del trattamento stesso che – ovviamente – non può considerarsi *personale* o *domestico* ma espressamente teso all'adempimento degli obblighi di comunicazione gravanti sulla pubblica amministrazione.

Sul punto vale la pena di osservare che l'esame di alcune pagine istituzionali di alcuni enti pubblici ha evidenziato la tendenza ad operare un mero rinvio alla *privacy policy* in uso sulle piattaforme, rimando che pare inadeguato o, comunque, insufficiente[67]. Nell'ipotesi che l'ente assuma la veste di titolare del trattamento, allora su di esso graveranno tutti gli obblighi previsti dall'ordinamento e si dovrà quindi procedere con tutte le attività necessarie a rispettare quanto previsto dal GDPR[68], tra cui il principio di trasparenza e accountability e, pertanto, predisporre l'informativa.

Dal riconoscimento dello *status* di titolare del trattamento in capo all'ente pubblico gestore di una pagina istituzionale deriva una serie di interrogativi che discendono da tre fattori: *i*) la sua natura di ente collettivo (che necessita pertanto di esternare le proprie decisioni con atti amministrativi); *ii*) le concrete modalità con cui le piattaforme consentono l'apertura delle pagine degli enti pubblici (in maniera "mediata" attraverso l'utilizzo di un account privato); *iii*) la natura fattuale che il GDPR attribuisce al titolare.

In altri termini: il GDPR attribuisce la funzione di *data controller* al soggetto che, in concreto, ha esercitato un'influenza effettiva in ordine alla determinazione dei fini e dei mezzi del trattamento[69]. Quindi l'ente assume la qualifica di titolare non solo allorché abbia esercitato il suo potere di decisione in merito alla scelta di aprire un account social, ma anche in quanto abbia effettuato la scelta di quali funzionalità attivare (o disattivare), fornendo istruzioni scritte e dettagliate al dipendente che sia titolare dell'account privato utilizzato per aprire la pagina istituzionale.

Ma se il dipendente incaricato di aprire la pagina non dovesse seguire le indicazioni fornite dall'ente, diverrebbe egli stesso titolare del trattamento per aver esercitato un'influenza effettiva sulle modalità di trattamento? La risposta pare dover essere affermativa, con evidenti ripercussioni sul dipendente che si vedrà gravato degli obblighi previsti dal GDPR e delle relative responsabilità, in applicazione del principio di responsabilizzazione del soggetto che abbia effettivamente concorso con altri nelle decisioni concernenti finalità e modalità di un trattamento.

La predisposizione di un mandato scritto che contenga in maniera dettagliata le istruzioni impartite dall'amministrazione delegante al proprio dipendente, oltre a costituire un opportuno presidio avverso le possibili contestazioni del dipendente (come si è già avuto modo di accennare al par. 5), si rivela anche una misura organizzativa che, nell'ottica di accountability, consente all'amministrazione di evitare che l'attività di comunicazione tramite social sia connotata, sin dall'inizio, da un'illegittimità sotto il profilo del rispetto del GDPR.

Nella diversa ipotesi in cui l'ente si avvalga di un soggetto esterno, al quale sia stato conferito l'incarico di gestire la pagina istituzionale[70], l'amministrazione dovrebbe provvedere ad effettuare la nomina di tale soggetto quale responsabile del trattamento (*data processor*) con il rispetto delle forme previste dall'art. 28 del GDPR.

8. La necessità di prevedere una *social media policy* interna ed esterna

La complessità delle interazioni che avvengono sulle piattaforme di social network che, come si

67. Osservazione già effettuata da Zunarelli-Alvisi 2020.
68. A titolo esemplificativo e non esaustivo: pianificare ed adottare adeguate misure tecniche e organizzative, fin dal momento della progettazione dei trattamenti (*by design*), individuare la corretta base giuridica del trattamento e, qualora dovesse individuarsi nel consenso dell'interessato, fornire tutte le informazioni previste dagli artt. 13 e 14 GDPR, tra cui i dati di contatto del DPO (la cui nomina è obbligatoria per gli enti ai sensi dell'art 37.4 lett. a) GDPR), indicare le finalità del trattamento, il periodo di conservazione etc.
69. Si richiama, sul punto, il parere del «Gruppo di lavoro art. 29 per la protezione dei dati» n. 1/10 adottato il 16 febbraio 2010.
70. Non è infatti infrequente che le amministrazioni si rivolgano a social media manager o a web agencies che si occupano in maniera professionale di comunicazione tramite piattaforme.

è visto al par. 1.2, ha determinato il superamento della comunicazione monodirezionale tipica del cartaceo (o del sito web istituzionale) e l'ingresso nel cosiddetto web 2.0, comporta un impatto organizzativo notevole per la pubblica amministrazione che voglia approfittare a fondo delle opportunità messe a disposizione dalle nuove tecnologie. Non si tratta più, infatti, di gestire unicamente il processo di output (come una brochure, un sito web o una pubblicità) ma un processo che, essendo caratterizzato dall'interazione bidirezionale, deve considerare anche il feedback dell'utente.

È pertanto necessario normare i processi che regolano i rapporti con i cittadini che, potendo interagire direttamente con la pubblica amministrazione tramite i canali social istituzionali, assurgono dunque a veri e propri protagonisti dell'informazione pubblica.

Per fronteggiare questa esigenza ed affrontare in maniera prudente l'articolato e poliedrico mondo dei social network, la PA deve preventivamente munirsi di un apparato regolamentare che funga da guida per i dipendenti che poi dovranno operativamente gestire il profilo istituzionale.

Sia il *Vademecum "Pubblica amministrazione e social media"* del 2009, sia il più recente e-book curato da FormezPA in collaborazione con PAsocial[71], forniscono dei suggerimenti sul contenuto dei provvedimenti interni con cui il singolo ente deve definire le regole per l'utilizzo dei social[72], sia in relazione ai profili interni all'ente sia in relazione ai profili esterni nei confronti dei cittadini.

La *social media policy* interna è il documento che definisce le regole di gestione della comunicazione tramite social ed è diretto al personale interno all'ente.

Tale documento deve fornire indicazioni generali sulle modalità della presenza in rete dell'amministrazione (le regole di comportamento dei dipendenti, le modalità d'interazione con i cittadini e la "filosofia"[73] sottesa alla presenza dello specifico ente in rete) ma anche regole specifiche legate ai contenuti: ad esempio, tipologia di contenuti pubblicabili (immagini, video, oppure solo testo) e quale tipo di licenza utilizzare (*creative commons* etc.).

Dovranno inoltre essere procedimentalizzate le modalità di gestione degli account pubblici e dovranno essere individuati i soggetti responsabili, così da rendere chiari i ruoli e le relative responsabilità; inoltre, l'amministrazione dovrà fornire le "regole d'ingaggio" nei rapporti con il pubblico e le modalità di risposta, oltre che lo stile di relazione da intrattenere con gli utenti.

In aggiunta alle norme dedicate a disciplinare l'attività di chi utilizza l'account istituzionale in nome e per conto dell'ente, non dovranno poi mancare indicazioni sulle modalità di utilizzo dei propri account personali: andrà disciplinata innanzitutto la possibilità di utilizzare i social personali durante l'orario di lavoro[74], ma andrà inoltre evidenziato che la persona può essere identificata dagli altri utenti come dipendente della PA anche allorquando interagisce con il proprio account privato fuori dell'orario di lavoro.

Proprio in funzione di questa riconducibilità delle attività private al proprio ente, al dipendente andrà innanzitutto ricordato il rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione (d.P.R. 62/2013) e, ove esistente, anche del Codice di comportamento adottato dal singolo ente in forza dell'art. 54, comma 5 del TUPI, ma potranno essere adottate anche regole specifiche mirate a meglio descrivere le condotte e a circoscrivere le responsabilità conseguenti l'utilizzo dei social media[75].

La *social media policy* esterna è rivolta, invece, ai cittadini/utenti e contiene le regole di comportamento da tenere negli spazi di presidio dell'ente: indica insomma quali contenuti e quali modalità di relazione ci si deve aspettare dall'ente nelle piattaforme social.

Ciò è oltremodo opportuno se si considera che la possibilità offerta dall'interazione bidirezionale

71. Talamo-Di Costanzo-Crudele 2017.
72. Per un esame più approfondito si rimanda a Faini 2017, p. 340 ss.
73. La locuzione "filosofia di presenza in rete" è utilizzata da FormezPA 2009.
74. Aspetto che si è rivelato particolarmente problematico dal momento in cui tutti si sono dotati di potenti smartphone che consentono di essere sempre connessi alla rete.
75. Alcune amministrazioni hanno scelto di inserire nella social media policy interna l'invito ad astenersi dal parlare di problemi di lavoro mediante i social network.

tipica dei social network consente a chiunque di inviare segnalazioni di disservizi, ma anche manifestazioni di dissenso rispetto a scelte amministrative oppure apprezzamenti negativi sugli amministratori.

Proprio al fine di prevenire situazioni sconvenienti o – peggio ancora – possibili contenziosi, è necessario che l'amministrazione predisponga e metta a disposizione degli utenti un documento che indichi in modo chiaro:

- l'ente o ufficio che gestisce lo spazio;
- le finalità perseguite dall'Amministrazione sul social network;
- il tipo di contenuti che sono pubblicati e, quindi, quali sono gli argomenti e i temi dei quali si può dibattere nello spazio virtuale dell'ente, il tipo di materiale che l'utente si può aspettare di trovare in tale contesto, chi può contribuire a incrementarlo e in che modo;
- quali sono i comportamenti consentiti: quale è la relazione che si vuole sviluppare con il cittadino, quali commenti e argomenti sono accettati e come sono gestiti i commenti non coerenti con i temi trattati (*off topic* e *spam*) o che adottano un linguaggio inappropriato;
- l'informativa ai sensi della normativa in materia di riservatezza dei dati personali (di cui si è detto *supra* al par. 7);
- gli ulteriori contatti dell'ente diversi dal social network (posta elettronica, numeri di telefono o indirizzo del sito internet istituzionale).

L'elencazione sopra riportata è contenuta nel *Vademecum*[76], ed è finalizzata a rendere più semplice e trasparente la gestione degli spazi virtuali, riducendo al minimo il rischio di critiche e malintesi durante l'interazione con cittadini/utenti.

Inoltre la pubblica amministrazione deve anche preoccuparsi che gli utenti non violino le condizioni di utilizzo delle varie piattaforme, posto che – come accennato al par. 3 – la PA è tenuta a rispettare il contenuto dei *terms and conditions* che (più o meno consapevolmente) ha accettato al momento della creazione del profilo pubblico. Pertanto la *social media policy* esterna dovrà contenere anche un'apposita raccomandazione al rispetto delle condizioni di utilizzo del servizio di ogni singola piattaforma (ad es., riguardo al divieto di pubblicazione di immagini oscene o di contenuti coperti dal diritto d'autore).

9. Conclusioni

L'utilizzo dei social network da parte delle pubbliche amministrazioni, quantunque non costituisca un obbligo normativo, rappresenta un'imperdibile occasione per conseguire gli obbiettivi di trasparenza ed efficacia amministrativa imposti dall'ordinamento, oltre che il raggiungimento della massima partecipazione dei cittadini.

Il mondo della comunicazione digitale (*rectius* telematica) è però costellato da numerose criticità legate, alcune, alla natura stessa delle piattaforme utilizzate ed altre alle tipicità che caratterizzano l'operare della pubblica amministrazione.

È quindi necessario che la pubblica amministrazione presti attenzione ai seguenti profili:

- al rispetto della normativa che disciplina i plurimi aspetti coinvolti dalla comunicazione pubblica ed in particolare: le disposizioni che disciplinano la comunicazione pubblica (l. 7 giugno 2000, n. 150), la normativa in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e Regolamento Ue n. 2016/679 - GDPR), le disposizioni per favore l'accesso dei soggetti disabili agli strumenti informatici (l. 9 gennaio 2004, n. 4), il Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82); il nuovo Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36);
- alla natura necessariamente partecipativa dei social, in cui gli utenti interagiscono in maniera diretta con la pubblica amministrazione;
- alla natura giuridica del contratto di social network e alle conseguenze che ne discendono in ordine ai diversi regimi di responsabilità che derivano dall'applicazione delle condizioni imposte dalle piattaforme;
- alle procedure previste dalle piattaforme che consentono l'apertura di profili pubblici solamente attraverso l'utilizzo di un profilo personale collegato ad una persona fisica;
- alla necessità d'individuare più di un soggetto a cui delegare tutti i poteri gestori del profilo pubblico;
- alla necessità di disciplinare in maniera dettagliata le modalità operative dell'utilizzo della pagina pubblica.

76. FormezPA 2009.

Per superare le criticità sopra indicate la pubblica amministrazione dovrà pertanto:

- predisporre in maniera ragionata un piano di comunicazione che tenga conto di tutte le norme che, a vario titolo, s'innestano nell'attività di comunicazione;
- coinvolgere tutti i soggetti all'interno della singola amministrazione che, ognuno per il proprio profilo di competenza, svolgono ruoli coinvolti dalla comunicazione digitale (responsabile della comunicazione, responsabile della transizione digitale, responsabile dei servizi informatici etc.);
- individuare un dipendente che dovrà prestare il consenso all'utilizzo del proprio profilo personale per creare la pagina pubblica dell'ente, munendolo dei necessari poteri per gestire in maniera trasparente, e sotto la supervisione dell'ente, il profilo pubblico;
- creare un una "catena di controllo" composta da diversi soggetti muniti dei necessari privilegi per gestire la pagina istituzionale anche in caso di impossibilità del soggetto incaricato;
- predisporre una *social media policy* interna che disciplini in maniera dettaglia le modalità di utilizzo dei social da parte di tutti i dipendenti;
- predisporre una *social media policy* esterna che disciplini i rapporti con gli utenti e che fornisca ai soggetti interni all'amministrazione tutte le indicazioni necessarie per relazionarsi in maniera adeguata e, soprattutto, rispettosa delle norme applicabili agli enti pubblici con i cittadini.

Riferimenti bibliografici

F. Astone (2011), *Il rapporto tra gestore e singolo utente: questioni generali*, in "Annali Italiani del Diritto d'Autore", 2011

E. Carloni (2013), *Il nuovo codice di comportamento ed il rafforzamento dell'imparzialità dei funzionari pubblici*, in "Istituzioni del federalismo", 2013, n. 2

European Data Protection Board (2021), *Linee guida 8/2020 sul targeting degli utenti di social media*, versione 2.0, 13 aprile 2021

F. Faini (2017), *Social open government: l'utilizzo dei social media nell'amministrazione digitale e aperta*, in "Informatica e diritto", 2017, n. 1-2

FormezPA (2009), *Vademecum "Pubblica Amministrazione e social media"*, 2009

G. Marino (2018), *La successione digitale*, in "Osservatorio del Diritto Civile e Commerciale", 2018

E. Montagnani (2021), *La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia: quali prospettive future?*, in "Rivista italiana di informatica e diritto", 2021, n. 1

C. Perlingieri (2018), I contratti tra Social Networks e utenti e il reimpiego dei dati di navigazione, in "Filodiritto", novembre 2018

C. Perlingieri (2014), *Profili civilistici dei social networks*, Edizioni Scientifiche Italiane, 2014

P. Rescigno (2000), *Manuale del diritto privato*, Ipsoa, 2000, p. 271

S. Rossa (2020), *L'impiego dei social network nella pubblica amministrazione: quid iuris?*, in "MediaLaws. Rivista di diritto dei media", 2020, n. 1

S. Talamo, F. Di Costanzo, R. Crudele (a cura di) (2017), *Social Media e PA, dalla formazione ai consigli per l'uso. Il primo libro "in progress" della nuova comunicazione pubblica*, 2017

S. Zunarelli, C. Alvisi (2020), *Studio inerente l'utilizzo e la gestione delle pagine istituzionali dei siti di social network delle PP.AA. e i riflessi sulla tutela della par condicio*, Corecom Emilia Romagna, febbraio 2020

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0116 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Paolo Caldarone

Il phishing bancario: principali strumenti di difesa e profili di responsabilità

Il contributo analizza la truffa informatica a danno degli istituti bancari, soffermandosi sui principali sviluppi giurisprudenziali e normativi compiuti dal legislatore comunitario e nazionale in materia di sicurezza delle nuove modalità di pagamento elettronico, concludendo con i diversi profili di responsabilità di *phisher* e financial manager.

Truffa informatica – Phishing – Sicurezza cibernetica – Dati personali

Banking phishing: main defense tools and responsibility profiles

The paper analyzes computer fraud to the detriment of banking institutions, focusing on the main case law and regulatory developments made by the EU and Italian legislation about new electronic payment methods security. In conclusion, different profiles of responsibility of phisher and financial manager are discussed.

Fraud – Phishing – Cybersecurity – Personal data

L'Autore è praticante avvocato e tirocinante *ex* art. 73 DL 69/2013 presso la Procura generale della Corte suprema di cassazione

1. Introduzione

Il presente lavoro concentra la propria attenzione sul *phishing* bancario nelle operazioni di pagamento elettronico a distanza, evidenziando i principali strumenti di attacco per l'accesso agli account sulla piattaforma di *internet banking* e le rispettive misure di sicurezza, concludendo con i diversi profili di responsabilità, tra cui quella dell'istituto bancario nei confronti del titolare di un conto corrente vittima di truffa informatica.

In particolare, il contributo si articolerà in tre parti. La prima sarà dedicata ad alcune considerazioni a carattere generale concernenti l'incessante aumento di incidenti cibernetici a livello mondiale e la presa di posizione del legislatore europeo, mediante l'introduzione di nuove misure di sicurezza e regole uniformi attraverso, soprattutto, le direttive PSD, PSD2, NIS 1 e la nuova NIS 2, e il loro recepimento dal legislatore nazionale, con l'obiettivo di incrementare le tutele dei consumatori nei c.d. pagamenti digitali all'interno dell'Eurozona. Nella seconda parte verranno analizzate le diverse tipologie di reati informatici a danno degli istituti bancari, specialmente i delitti di accesso abusivo ai sistemi informatici e telematici, nonché la truffa informatica e i suoi principali elementi distintivi rispetto al delitto di furto e di truffa, sia dal punto di vista normativo che giurisprudenziale, evidenziando le diverse lacune che sono state lasciate dal legislatore nazionale, in parte risolte con i molteplici interventi del giudice nomofilattico e dell'Arbitro Bancario e Finanziario. La terza parte, invece, si concentrerà sui diversi profili di responsabilità tra il *financial manager* e il *phisher* ravvisabile sia nel concorso di persone, nel caso in cui il direttore finanziario, consapevole dell'attività del c.d. "truffatore informatico" collabori con quest'ultimo aprendo un conto nuovo o mettendo a disposizione il suo personale per il trasferimento del provento illecito, sia nel concorso di reato con il delitto di riciclaggio, evidenziando gli interventi dell'ABF e della Cassazione in materia.

Le premesse di fondo consistono nel cercare di apportare chiarezza in una tematica in continua evoluzione e novità, cercando dove possibile, di evidenziare le soluzioni ricercate dagli studiosi nelle situazioni di conflittualità normative sia sostanziali che processuali da cui è caratterizzata la suddetta materia, poiché riguardano strumenti e tecnologie informatiche che mutano giorno per giorno, rendendo, pertanto, anche le condotte criminose del soggetto agente di difficile regolamentazione e inquadramento per garantire un corretto esercizio dell'azione penale.

2. L'introduzione e gli obiettivi della *Payment Services Directive* – PSD2 e le principali misure di sicurezza a tutela del cliente: lo *strong customer authentication*

L'incessante evoluzione delle moderne tecnologie informatiche e telematiche ha avuto una grande influenza anche nel settore bancario, estendendo le modalità di pagamento dell'utente, dal mondo reale alla dimensione digitale, attraverso sia l'utilizzo dello smartphone con la tecnologia NFC (*Near Field Communication*)[1], i sistemi Internet/WAP, il servizio SMS (*Smart Message Service*) a tariffazione maggioritaria e addebiti al pagatore per mezzo del gestore del servizio telefonico, sia i c.d. pagamenti elettronici che comprendono i pagamenti con carta a distanza attraverso l'invio dei dati via internet, la moneta elettronica[2] e i bonifici o addebiti diretti tramite il servizio di *internet banking*[3], sviluppato alla fine degli anni Ottanta, e consiste in un sistema che consente al cliente l'accesso ai servizi bancari attraverso la rete[4].

Numerosi e in costante aumento sono i gravi incidenti cibernetici, a cui la stampa ha dato risalto, e i più clamorosi hanno riguardato: il sovraccarico di lavoro del software di una nota banca di New York, generando, di conseguenza, problematiche relative alla consegna agli acquirenti dei titoli governativi ricevuti dai venditori certificati del Tesoro e attribuendo la responsabilità, per la mancata ricezione degli investimenti, in capo all'istituto bancario che fu costretto a richiedere un prestito, al tasso di interesse del 7,5% alla *Federal Reserve Bank*; e il blocco informatico del 1987, avvenuto al Centro informatico della *Federal Reserve Bank*, che impedì per un giorno intero sia le grandi transazioni interbancarie, causando un aumento del tasso d'interesse dal 7% al 30%, sia la disponibilità di liquidità per le grandi banche, determinando una ricerca disperata del contante da parte degli operatori bancari[5].

Negli ultimi anni il legislatore europeo è intervenuto nella regolamentazione dei servizi di pagamento con la direttiva 2007/64/CE[6] (la c.d. PSD[7] - *Payment Service Directive*), che ha consentito alle istituzioni europee di fondare un mercato unico europeo dei pagamenti al dettaglio (c.d. SEPA – *Single Euro Payment Area*), e con la più recente direttiva 2015/2366/UE[8] (la c.d. PSD2[9]), che ha

1. Rappresenta una tecnologia wireless che consente lo scambio di informazioni e la effettuazione di pagamenti tra due telefoni cellulari abilitati NFC quando si toccano o si avvicinano, attraverso un sistema di radiofrequenza (RFID), Jain-Dahiya 2015.
2. Disciplinata dal Parlamento europeo e dal Consiglio nella direttiva 2009/110/CE, che la definisce nell'art. 2 come «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica», direttiva 2009/110/CE del Parlamento europeo e del Consiglio concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE.
3. Pascuzzi 2020, pp. 149-153.
4. Mukhtar 2015, pp. 1-5.
5. Sarzana 2010, pp. 15-17.
6. Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE.
7. Il nostro ordinamento ha recepito la suddetta direttiva con il d.lgs. n. 11 del 27 gennaio 2010 "Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE".
8. Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.
9. L'Italia ha recepito la fonte europea con il d.lgs. n. 218 del 15 dicembre 2017, "Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE,

integrato il quadro normativo precedente, adeguandolo al fenomeno della *digital revolution*[10].

Più precisamente, l'intenzione del legislatore comunitario con la PSD è stata quella di disporre regole uniformi, fondate sulla trasparenza e sicurezza a tutela del consumatore, per promuovere l'utilizzo dei pagamenti elettronici e innovativi in tutta l'Eurozona, riducendo il costo di strumenti quali quelli cartacei e il contante; tuttavia, suddetta fonte unionale si è dimostrata inadeguata al fenomeno dell'*open banking*[11], che ha portato nuovi prestatori di servizi, operanti al di fuori dell'ambito bancario, e alle nuove modalità di pagamento, necessitando di strumenti di sicurezza più rigidi a tutela dei consumatori, determinando l'introduzione della direttiva PSD2.

Le nuove misure di sicurezza, finalizzate a ridurre il rischio che si verifichino operazioni di pagamento non autorizzate dall'utente, introdotte dalla direttiva, impongono la c.d. autenticazione forte (*Strong Customer Authentication*), una procedura finalizzata a verificare l'identità dell'utente e la validità dell'uso di uno specifico sistema di pagamento basata, ai sensi dell'art. 4 n. 30 della direttiva PSD2, «sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione»[12].

L'ambito di applicazione della nuova direttiva non si riferisce più soltanto ai classici enti creditizi e Istituti di Pagamento (IP), ma si estende anche a Banche, Istituti di Moneta Elettronica (IMEL), imprese diverse da quest'ultimi, autorizzati a prestare i servizi di pagamento dall'Autorità di Vigilanza che consentono di ampliare, sfruttando le potenzialità delle nuove tecnologie (come ad esempio: smartphone), il settore dei pagamenti elettronici[13].

3. La truffa informatica e la sua apparente similitudine al delitto di furto e di truffa: la classificazione del *phishing* nel diritto interno e la principale tecnica di attacco informatico nel settore bancario

Nello scenario attuale e ancor di più nel futuro, dove la quasi totalità delle azioni umane sfruttano e sfrutteranno innumerevoli servizi digitali, interconnessi e comunicanti, la truffa informatica è divenuta, pariteticamente all'implementazione di misure sempre più efficienti ed efficaci per la mitigazione del rischio *cyber*, un fenomeno criminoso ontologicamente in evoluzione e difficile da classificare, in quanto sono molteplici le tecniche con cui viene messa in atto; ciononostante, sono tutte accomunate dall'influenza psicologica sulla vittima e dalla strumentalizzazione dell'identità digitale di un soggetto, con finalità di ingiusto profitto.

Tale trasformazione digitale e i rischi, che si concretizzano in attacchi molto più devastanti di quelli visti fino ad ora, hanno avuto conseguenze anche in ambito penale, aprendo un forte dibattito tra gli studiosi per individuare la "giusta" tutela normativa dei nuovi beni giuridici informatici e, in rapporto alla *quaestio iuris*, due sono state le

2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta".

10. Il suddetto fenomeno ha portato alla nascita della c.d. Fintech, che semanticamente deriva dall'unione della parola "finanza" e "tecnologia" ed è traducibile in "tecnologia applicata alla finanza" e consiste in un ampio insieme di innovazioni che sono rese possibili dall'impiego delle nuove tecnologie sia nell'offerta di servizi agli utenti sia nei processi produttivi interni agli operatori finanziari, D'Agostino-Munafò 2018, p. VIII.
11. Consiste in un nuovo modello bancario che garantisce alle terze parti, fornitrici di servizi finanziari (TPP), un accesso libero a servizi bancari, transazioni e altri dati finanziari dei clienti tramite l'uso di interfacce tecnologiche intertemporali API (*Application Programming Interface*), rimuovendo l'esclusiva concentrazione delle informazioni finanziarie in capo alle banche tradizionali e consentendo la condivisione di dati e conti, Ferretti 2021, p. 4.
12. Sica-Sabatino 2021, pp. 1-4.
13. Olivieri 2021, pp. 450-454.

soluzioni: introdurre nuove fattispecie criminose o utilizzare norme già esistenti, adattandole, per via interpretativa, alle nuove esigenze.

Sebbene in un primo momento le c.d. truffe online siano state ricondotte all'art. 640 c.p.[14], per evitare sia forzature interpretative che la violazione del principio di legalità, in quanto alcuni comportamenti non potevano essere ricondotti alle fattispecie tradizionali[15], successivamente, il legislatore nazionale ha disciplinato, con la legge n. 547 del 23 dicembre 1993[16] e rispettive modifiche, il delitto di truffa informatica nell'art. 640-*ter* c.p.[17] individuando come oggetto di tutela il patrimonio del soggetto danneggiato, la regolarità del funzionamento del sistema telematico e informatico e, infine, la riservatezza nel suo utilizzo[18].

Dal punto di vista classificatorio, i reati informatici comprendono sia quelli commessi mediante l'uso delle tecnologie informatiche sia quelli in danno alle tecnologie stesse; inoltre, la dottrina ha distinto i reati commessi su Internet, riconducendo tutti quei crimini che non potrebbero essere attuati in assenza delle tecnologie informatiche, dai reati commessi attraverso Internet, intendendo la rete come mero strumento di supporto per la realizzazione dell'illecito e, di conseguenza, riferendosi ai c.d. reati tradizionali già contemplati nel codice penale e nelle leggi speciali[19].

La forma più comune di attacco informatico è quella del *deceptive phishing*, ossia il c.d. "phishing[20] ingannevole", in cui il truffatore si appropria di tutti i codici bancari dell'utente, condizionandolo a cliccare, attraverso l'invio di una email piuttosto similare a quella dell'istituto bancario, su un link, oggetto del messaggio, che lo indirizzerà ad una pagina web, pressoché identica a quella del sito ufficiale, dove dovrà inserire tutte le informazioni necessarie per accedere all'*internet banking*[21].

14. Cfr. Alibrandi-Corso 2022, p. 315. Nel delitto di truffa «Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità; 2-*bis*. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente».
15. Bartoli-Pelissero-Seminara 2020, pp. 331-333.
16. Legge 23 dicembre 1993, n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
17. Cfr. Alibrandi-Corso 2022, pp. 315-316. Ai sensi dell'articolo in esame la frode informatica punisce «Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età».
18. Bartoli-Pelissero-Seminara 2020, pp. 333-334.
19. Circelli 2015, pp. 132-133.
20. In particolare, il *phishing* è una truffa attraverso la quale si persuade il destinatario con la simulazione di messaggi elettronici di noti fornitori di servizi, per ottenere informazioni riservate dell'utente, D'Agostino-Panebianco 2020, p. 242.
21. Cipolla 2012, pp. 2686-2688.

Dal punto di vista definitorio, si è pronunciato anche il giudice di legittimità al riguardo, definendo il *phishing* come «quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici c.d. *malware*) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati»[22].

In relazione alla struttura del reato di *phishing* si può individuare, apparentemente, una similitudine al delitto di truffa, in quanto ricomprende una moltitudine di condotte fraudolente idonee a conseguire un profitto e un danno alla vittima, e di furto, poiché l'aggressione è unilaterale; tuttavia, gli elementi distintivi in relazione al furto, consistono nella realizzazione dell'evento di profitto e di danno[23], mentre in rapporto alla truffa, mancano nella struttura oggettiva della condotta punibile sia l'induzione in errore della vittima sia gli artifici e i raggiri commessi dal soggetto agente, entrambi difficilmente realizzabili con una macchina, in quanto priva delle caratteristiche dell'essere umano[24]. Infatti, la Cassazione[25] ha precisato che «il reato di frode informatica si differenzia dal reato di truffa perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema». Tuttavia, come il reato di truffa, anche quella informatica prevede come elemento psicologico in capo al soggetto agente del reato, il dolo generico, consistente nella consapevolezza e nella volontà di procurare a sé o ad altri un profitto ingiusto con altrui danno, sulla base del risultato irregolare di un procedimento di elaborazione di dati, ottenuto mediante l'alterazione del sistema di funzionamento dell'elaboratore, ovvero intervenendo senza esserne autorizzati sui dati o sulle informazioni oggetto di trattamento[26].

Prima di analizzare la condotta incriminatrice del *reo*, è importante porre alcune definizioni semantiche: per sistema informatico si intende un sistema completo di apparecchiature di elaborazione composto sia da elementi hardware, sia da elementi software, funzionanti in reciproca implementazione; il sistema telematico, invece, è il complesso di elementi che costituiscono un'apparecchiatura per la trasmissione a distanza di dati; tuttavia, entrambi devono essere dotati di misure di sicurezza volte a selezionare ed individuare i soggetti abilitati all'accesso al sistema protetto[27].

Per quanto riguarda la condotta fraudolenta tenuta dall'autore del reato, questa può realizzarsi in qualsiasi modalità ma deve necessariamente consistere in un'alterazione di un sistema informatico o telematico, con modalità diverse, attraverso la quale gli schemi predefiniti del sistema vengono modificati o manipolati, al fine di perseguire un ingiusto profitto con l'altrui danno; ovvero, l'intervento, con qualsiasi modalità, sui dati, le informazioni o i programmi contenuti nel sistema, al fine di realizzare un ingiusto profitto con l'altrui danno[28].

La fattispecie criminosa in esame prevedeva, inizialmente, due ipotesi di circostanze aggravanti: la prima si riferiva essenzialmente al caso in cui il fatto veniva commesso ai danni dello Stato; la seconda, invece, al fatto commesso con abuso della qualità di operatore di sistema, una nozione atecnica in quanto comprende qualsiasi mansione che implichi l'attività di utilizzazione di un

22. Cass. pen., sez. II, sentenza 11 marzo 2011, n. 9891.

23. Bartoli-Pelissero-Seminara 2020, pp. 334-336.

24. Bartoli 2011, pp. 384-387.

25. Cass. pen., sez. II, sentenza 11 novembre 2009, n. 44720.

26. Dolcini-Gatta 2021, pp. 2668-2670.

27. Fiandaca-Musco 2020, pp. 362-365.

28. *Ivi*, pp. 205-207.

elaboratore[29]. Con la novella del 2021[30], il legislatore nazionale ha introdotto una nuova circostanza aggravante per il delitto di cui all'art. 640-*ter* c.p. nel caso in cui il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale, in risposta alla necessaria sanzione di suddetta condotta prevista dall'art. 6 della direttiva 2019/713/UE[31], contrapponendo la valuta virtuale a quella monetaria, senza, tuttavia, rispettare la specifica indicazione del legislatore europeo che, come specificato nell'art. 2 lett. d) della medesima direttiva, si concentra sulla tutela penale della sola valuta che abbia una certa diffusione sul mercato[32].

Dal punto di vista giurisprudenziale sono molteplici gli interventi da parte della Cassazione in materia di frode informatica, che hanno permesso di colmare diverse lacune applicative di suddetta fattispecie da parte del legislatore nazionale. In particolare, il giudice di legittimità con sentenza n. 47302/2021 ha escluso per la consumazione del delitto di truffa aggravata ai danni dello Stato, la condotta relativa alla sostituzione di schede "clonate" nelle slot machine che alterava il funzionamento del sistema informatico di suddette apparecchiature, impedendo la comunicazione dei dati delle giocate effettive all'Amministrazione finanziaria, in quanto costitutive del delitto di frode informatica[33].

Oltre a ciò, con sentenza n. 40862/2022, il giudice nomofilattico ha precisato, in relazione all'aggravante prevista all'art. 640-*ter* c.p., la portata applicativa della nozione di "identità digitale" applicandola anche per l'accesso alla piattaforma di *home banking* gestita da privati. In particolare, ha statuito che «in tema di frode informatica, la nozione di "identità digitale", che integra l'aggravante di cui all'art. 640-*ter*, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati»[34].

Giova, inoltre, indicare la recentissima sentenza n. 13713/2023 con cui la Corte di Cassazione ha chiarito che l'elemento specializzante del reato di cui all'art. 640-*ter* c.p. è rappresentato dall'utilizzazione fraudolenta del sistema informatico, poiché costituisce presupposto assorbente rispetto alla portata generica del delitto di indebita utilizzazione di carte di pagamento di cui all'art. 55, comma 9, d.lgs. 21 novembre 2007, n. 231. Infatti, ha statuito che «integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di pagamento di cui all'art. 55, comma 9, d.lgs. 21 novembre 2001, n. 231, la condotta di chi, servendosi di carte per l'erogazione di carburante in precedenza clonate, acceda ai sistemi informatici predisposti presso i relativi impianti, con successivo prelievo abusivo di carburante»[35].

Quest'ultima sentenza è risultata fondamentale, in quanto ha risolto le complicanze interpretativo-applicative a cui il quadro normativo è stato sottoposto con le integrazioni verificatesi mediante l'attuazione della direttiva 2019/713/UE nel nostro ordinamento, che faceva ritenere, l'uso di codici

29. Parodi 1997, pp. 1540-1545.

30. Art. 2 del d.l. 8 novembre 2021, n. 184, "Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio".

31. Infatti, l'articolo in questione prevede che «Gli Stati membri adottano le misure necessarie affinché l'atto di effettuare o indurre un trasferimento di denaro, di valore monetario o di valuta virtuale, arrecando illecitamente a terzi una perdita patrimoniale allo scopo di procurare un ingiusto profitto all'autore del reato o a una terza parte sia punibile come reato, se commesso intenzionalmente nel modo seguente: a) ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso; b) introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici», direttiva (UE) 2019/713 del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio.

32. Crescioli 2022, pp. 10-11.

33. Cass. pen., sez. II, sentenza 14 settembre 2021, n. 47302.

34. Cass. pen., sez. II, sentenza 20 settembre 2022, n. 40862.

35. Cass. pen., sez. II, sentenza 9 febbraio 2023, n. 13713.

e numeri di carte di credito clonate per penetrare abusivamente il sistema informatico bancario ed effettuare operazioni indebite, come condotta non soltanto integrativa del delitto di frode informatica, bensì anche realizzazione del delitto di indebita utilizzazione di carte di pagamento [36].

Gli interventi da parte della Cassazione non hanno riguardato, tuttavia, soltanto profili sostanziali di suddetta fattispecie criminosa, bensì anche alcuni aspetti processuali riguardo il giudice territorialmente competente. Infatti, in relazione a suddetto profilo, sebbene il giudice territorialmente competente in materia di truffa informatica sia molto difficile da identificare, soprattutto attraverso il criterio generale del *locus commissi delicti*, ai sensi dell'art. 8, comma 1, c.p.p., a causa della moneta elettronica che consente l'utilizzo della carta in qualsiasi sportello ATM (*Automated Teller Machine*) ed operazioni di bonifici on-line, il giudice nomofilattico ha chiarificato suddetta questione[37], attribuendo la competenza al giudice del luogo in cui si è verificata l'esecuzione dell'attività manipolatoria del sistema, spostando l'attenzione al momento e, non soltanto al luogo in cui l'autore dell'illecito consegue l'ingiusto profitto, con la conseguente *deminutio patrimonii* della vittima, mentre nel caso in cui l'operazione avvenga mediante i sistemi di trasferimento bancario on-line, il giudice di legittimità[38] si è pronunciato individuando come competente il giudice del luogo in cui il destinatario ha aperto il conto corrente presso l'istituto bancario[39].

Occorre, inoltre, evidenziare che da suddetta condotta emergono diversi profili di responsabilità inerenti il *data breach*[40] ed il principio di accountability[41], in capo al titolare del trattamento di dati e al suo specifico obbligo di istruzione e formazione; infatti, la Suprema Corte di Cassazione ha precisato che «in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema [il che rappresenta interesse degli stessi operatori], è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. Ne consegue che, anche prima dell'entrata in vigore del d.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente»[42].

4. I diversi profili di responsabilità tra *financial manager* e *phisher*: il concorso tra ricettazione e frode informatica, l'intervento dell'ABF e la recentissima sentenza della Cassazione n. 7214 del 2023

Nelle frodi informatiche ruolo centrale è rivestito dal *financial manager*, cioè colui che riceve, in accordo con il *phisher*, le somme sottratte

36. Crescioli 2022, p. 4.
37. Cass. pen., sez. II, sentenza 17 marzo 2020, n. 10354.
38. Cass. pen., sez. feriale, sentenza 8 settembre 2016, n. 37400.
39. Pecorella 2012, pp. 113-116.
40. Per violazione dei dati personali; il c.d. *data breach*, ai sensi dell'art. 4, n. 12 GDPR, è «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati», 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.
41. Introdotto proprio dal GDPR secondo il quale il titolare del trattamento deve adottare le misure adeguate ed attuare i principi e le disposizioni del regolamento conformemente alle caratteristiche specifiche del trattamento e comprovare di avere svolto suddetta attività, Finocchiaro 2022, p. 312.
42. Cass. civ., sez. I, sentenza 3 febbraio 2017, n. 2950.

indebitamente da quest'ultimo e le trasferisce, dopo aver ricevuto il proprio corrispettivo, dal proprio conto a terzi, attraverso l'utilizzo delle piattaforme che svolgono in necessari servizi.

In relazione alla condotta tenuta dal direttore finanziario si possono configurare due profili criminologici: da un lato, sussiste il concorso, ai sensi dell'art. 110 c.p., nel delitto di frode informatica, nel caso lo stesso sia consapevole dell'attività illegale compiuta dal *phisher*, tanto da assicurarne la propria collaborazione; dall'altro, nel caso in cui, lo stesso non è a conoscenza della condotta ma comunque mette a disposizione il proprio conto per il trasferimento del provento illecito – o ne apre uno a tal fine – e successivamente, trasferisce denaro a terzi, risponde di ricettazione o riciclaggio, a titolo di dolo eventuale[43].

Dal punto di vista giurisprudenziale sono molteplici le pronunce che non riconoscono un concorso di reati tra frode informatica e riciclaggio nei confronti del *financial manager*[44], mentre altre[45] sostengono che risponde, nel caso in cui il medesimo è consapevole della frode e assicura la propria collaborazione, di concorso nell'attività delittuosa, senza commettere ulteriori crimini[46]. Più precisamente, in quest'ultima ipotesi il dolo di ricettazione sussiste solo nel caso in cui, in base a precisi elementi di fatto, il direttore finanziario si sia rappresentato l'eventualità che le somme di denaro trasferite derivano da attività illecita e ne abbia comunque trasferito a terzi i proventi[47].

Inizialmente, sul profilo di responsabilità tra il *financial manager* e l'autore della frode informatica, in mancanza di interventi della giurisprudenza di legittimità e del legislatore nazionale, si è espresso l'Arbitro Bancario Finanziario[48] (ABF)[49], sebbene tali decisioni siano prive di vincolatività rispetto alle pronunce giurisprudenziali, tuttavia, devono essere rispettate dall'intermediario finanziario. In particolare, le decisioni del Collegio di coordinamento nn. 3498/2012[50] e 1820/2013 hanno distinto le truffe informatiche in ipotesi di *phishing* tradizionale via email, telefonico (c.d. *vishing*) e via SMS (c.d. *smishing*) con il quale si invita il cliente a digitare le proprie credenziali di acceso su una piattaforma di *internet banking* simile a quella ufficiale[51].

Inoltre, la decisione n. 1820/2013 ha sancito che nel caso di specie, il prelievo fraudolento effettuato sul conto corrente del cliente mediante bonifico non autorizzato è dipeso dalla negligenza di quest'ultimo, poiché la frode è stata attuata con modalità note dai consociati e di immediata riconoscibilità anche per un utente non esperto, dato che il messaggio email del *phisher* era inviato da un indirizzo assolutamente generico, redatto con un

43. Di Paolo 2017, pp. 14-19.

44. In particolare, la Cassazione ha precisato che «Nel phishing (truffa informatica effettuata inviando una email con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati quali numero di carta di credito, password di accesso al servizio di *home banking*, motivando tale richiesta con ragioni di ordine tecnico), accanto alla figura dell'hacker (esperto informatico) che si procura i dati, assume rilievo quella collaboratore prestaconto che mette a disposizione un conto corrente per accreditare le somme, ai fini della destinazione finale di tali somme. A tal riguardo, il comportamento di tale soggetto è punibile a titolo di riciclaggio ex art. 648-*bis* c.p., e non a titolo di concorso nei reati con cui si è sostanziato il *phishing* (art. 615-*ter* e 640-*ter* c.p.), giacché la relativa condotta interviene, successivamente, con il compimento di operazioni volte a ostacolare la provenienza delittuosa delle somme depositate sul conto corrente e successivamente utilizzate per prelievi di contanti, ricariche di carte di credito o ricariche telefoniche», Cass. pen., sez. II, sentenza 9 febbraio 2017, n. 10060.

45. Cass. pen., sez. II, sentenza 17 giugno 2011, n. 25960.

46. Reccia 2022, pp. 13-20.

47. Piancastelli 2015, pp. 6-7.

48. Per approfondire si segnala: Muttini 2021, pp. 41 ss.

49. L'ABF è un sistema di risoluzione stragiudiziale, alternativo, più rapido e meno costoso della giustizia ordinaria, competente per le controversie che possono nascere tra i clienti, le banche e gli intermediari finanziari ed è attivo dal 2009, Morera 2023, pp. 24-26.

50. Arbitro Bancario Finanziario, decisione 26 ottobre 2012, n. 3498.

51. Calisai 2015, pp. 83-85.

italiano approssimativo, con errori lessicali e grammaticali e, pertanto, non sussiste alcuna responsabilità in capo all'intermediario finanziario[52].

È opportuno precisare che, ai sensi dell'art. 9, comma 1, del d.lgs. 27 gennaio 2010, n. 11 (novellato dalla direttiva PSD2), si considera contestata l'operazione disconosciuta dal cliente nel termine di 13 mesi dalla data di addebito[53].

Per quanto riguarda gli oneri probatori in capo alla banca, gli viene richiesto di dimostrare la corretta autenticazione del cliente sul sito di *internet banking*, attraverso la produzione dei c.d. log, nonché la colpa grave dell'utente, ossia l'esistenza di un comportamento abnorme, non scusabile del cliente[54].

In particolare, la recentissima sentenza n. 7214, pubblicata il 13 marzo 2023, della Cassazione Civile ha escluso il risarcimento per il correntista rimasto vittima di *phishing*, introducendo, conseguentemente, un principio che rappresenta per gli istituti di credito uno "scudo" di fronte a suddette richieste di risarcimento danni dei truffati online, mentre per i correntisti una maggiore responsabilizzazione nell'uso dei codici personali e dichiarando che «non può dubitarsi del comportamento decisamente imprudente e negligente del danneggiato, il quale aveva digitato i propri codici personali (verosimilmente richiestigli con una e-mail fraudolenta), in tal modo consentendo all'ignoto truffatore di utilizzarli successivamente, per effettuare una disposizione di bonifico dal conto del danneggiato (esclusa, nella specie, la restituzione delle somme prelevate da un conto corrente mediante bonifico online, atteso che la responsabilità era da addossarsi al danneggiato che aveva incautamente fornito i propri codici personali verosimilmente a causa di un'attività di *phishing*)». Nel caso di specie, l'esclusione della responsabilità di suddetto istituto di credito è dipesa dalla condotta colposa dell'utente, che ha determinato l'addebito della somma, consistente in un comportamento imprudente e negligenze poiché l'utente ha digitato, contrariamente a quanto indicato nel foglio informativo, nonché nei messaggi pubblicitari *anti-phishing* sul sito internet di Poste italiane S.p.A., che forniscono le necessarie informazioni per evitare frodi informatiche, i propri codici identificativi personali senza alcuna precauzione nella loro custodia e nel loro corretto utilizzo[55].

Con quest'ultima sentenza si può certamente constatare il recepimento della soluzione evidenziata dall'ABF in materia di esclusione di responsabilità della banca se il titolare del conto corrente è stato negligente, nel caso in cui la truffa di cui è stato vittima sarebbe stata immediatamente riconosciuta anche per un utente non esperto, se avesse seguito la c.d. informativa anti-truffa pubblicizzata dall'istituto di credito.

5. Considerazioni conclusive

In relazione a quanto riportato, sono stati fondamentali gli interventi di chiarificazione dell'ABF, seppure non vincolanti, in rapporto ai profili di responsabilità in materia di *phishing* e dei particolari oneri probatori in capo agli istituti di credito, a causa delle ampie lacune normative lasciate dal legislatore.

A tal riguardo, come visto, un chiarimento deriva dalla recentissima sentenza della Cassazione Civile n. 7214 del 13 marzo 2023 che ha escluso il risarcimento del danno degli utenti truffati verso gli istituti bancari, se questi fanno un uso imprudente e negligente dei codici personali di accesso, non seguendo le indicazioni pubblicitarie anti-frode delle banche, benché appaia palesemente insufficiente, in relazione alla effettiva tutela dell'utente, una sorta di "brochure" informativa per i correntisti sui rischi connessi al *phishing*; sarebbe, invece, necessaria una sorta di educazione digitale concreta dei rischi connessi all'utilizzo di queste piattaforme degli utenti più "deboli", come coloro che non appartengono ai c.d. nativi digitali, attraverso corsi formativi che spieghino in maniera chiara, immediata e, sempre

52. Arbitro Bancario Finanziario, decisione 5 aprile 2013, n. 1820.

53. Art. 9 del d.lgs. 27 gennaio 2010, n. 11, "Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE".

54. Minneci 2022, pp. 1052-1056.

55. Cass. civ., sez. I, sentenza del 13 marzo 2023 n. 7214.

in aggiornamento, le modalità, i rischi e gli strumenti per evitare le truffe informatiche.

Tuttavia, a causa dell'accrescimento delle frodi informatiche in Italia nel corso del 2022, dove sono state frodate 156 grandi, medie e piccole imprese, per un ammontare complessivo di oltre 20 milioni di euro di profitti illeciti, dei quali oltre 4 milioni di euro sono stati recuperati in seguito all'intervento della polizia postale e delle comunicazioni, si può stimare, in merito ai fenomeni di *phishing*, *smishing* e *vishing* un aumento di €. 5.419.752 delle somme sottratte, rispetto all'anno precedente.

In particolare, la causa principale dell'espansione del fenomeno di *financial cybercrime* è stata sicuramente l'emergenza sanitaria Covid-19 che ha comportato il cambiamento radicale di alcune abitudini di vita consolidate, ampliando l'utilizzo di tecnologie sia in ambito lavorativo, con lo *smart-working*, sia in ambito scolastico con l'utilizzo di piattaforme telematiche per lo studio[56]. Non si esclude a priori che suddetto fenomeno criminoso possa aumentare ulteriormente con i conflitti in corso, portando sicuramente il legislatore europeo e nazionale a introdurre ulteriori misure di sicurezza a tutela delle infrastrutture critiche.

Tuttavia, un ulteriore accrescimento di norme regolamentari in materia penale, come già avvenuto con la novella del 2021 sul reato di frode informatica, che il legislatore nazionale ha dovuto compiere per uniformarsi alla legislazione europea, risulta controproducente dal punto di vista applicativo sotto diversi aspetti, in quanto la novella non ha recepito correttamente, come evidenziato nei paragrafi precedenti, la direttiva 2019/713/UE in rapporto alla circostanza aggravante sancita nell'art. 640-*ter*, comma 3, c.p., non precludendo delle future contestazioni dalla Commissione europea; c'è inoltre una sovrapposizione di molteplici norme penali, facendo ricondurre ad un illecito contemporaneamente più incriminazioni diverse tra loro, rendendo necessario l'intervento chiarificatore del giudice di legittimità.

Si dovrebbe, pertanto, ridurre il carico normativo in materia penale, ed evitare il fenomeno del c.d. populismo penale introducendo sempre più fattispecie criminose, in quanto la funzione di suddetta materia deve essere preventiva e non limitarsi ad una operazione repressiva, soprattutto per crimini che sono in continua evoluzione, con un semplice aumento dei reati e, conseguentemente, attentando sempre più alla libertà personale, nonché compromettendo l'effettivo e corretto esercizio dell'azione penale.

Riferimenti bibliografici

L. Alibrandi, P. Corso (2022), *Codice penale e di procedura penale e leggi complementari*, La Tribuna, 2022

R. Bartoli (2011), *La frode informatica tra «modellistica», diritto vigente, diritto vivente e prospettive di riforma*, in "Il diritto dell'informazione e dell'informatica", 2011, n. 3

R. Bartoli, M. Pelissero, S. Seminara (2020), *Diritto penale. Lineamenti di parte speciale*, Giappichelli, 2020

F. Calisai (2015), *Il Phishing: profili civilistici ed evoluzione delle forme di tutela alla luce delle decisioni dell'Arbitro Bancario Finanziario*, in "Diritto Mercato Tecnologia", 2015, n. 2

P. Cipolla (2012), *Social network, furto di identità e reati contro il patrimonio*, in "Giurisprudenza di merito", 2012, n. 12

S. Circelli (2015), *I reati informatici*, in "La voce del foro", 2015

C. Crescioli (2022), *Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche*, in "Archivio Penale", 2022, n. 2

56. Polizia postale 2023.

G. D'Agostino, P. Munafò (2018), *Prefazione* alla collana dedicata al Fintech, in C. Schena, A. Tanda, C. Arlotta, G. Potenza (a cura di), "Lo sviluppo FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale", Quaderni FinTech, 1° marzo 2018

M. D'Agostino Panebianco (2020), *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in "Europa e Diritto Privato", 2020, n. 1

E. Dolcini, G.L. Gatta (2021), Codice penale commentato, Ipsoa, 2021

F. Ferretti (2015), *L'*open banking *e le troppe zone grigie del conflitto tra legislazione europea sui pagamenti e la tutela dei dati personali*, in "federalismi.it", 2021, n. 10

G. Fiandaca, E. Musco (2020), *Diritto penale. Parte speciale. I delitti contro il patrimonio*, Zanichelli, 2020

G. Finocchiaro (2022), *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in "Diritto dell'Informazione e dell'Informatica", 2022, n. 2

G. Jain, S. Dahiya (2015), *NFC: Advantages, limits and future scope*, in "International Journal on Cybernetics & Informatics" (IJCI), vol. 4, 2015, n. 4

U. Minneci (2022), *Pagamenti elettronici non autorizzati: la tutela del cliente alla luce degli orientamenti dell'ABF*, in "Giurisprudenza commerciale", 2022, n. 6

U. Morera (2023), *Il costo "zero", lo* jus variandi *e l'Arbitro Bancario Finanziario*, in "Banca borsa titoli di credito", 2023, n. 1

M. Mukhtar (2015), *Perceptions of UK Based Customers toward internet Banking in the United Kingdom*, in "Journal of Internet Banking and Commerce", 2015, n. 1

L. Muttini (2021), *Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'Arbitro Bancario Finanziario*, in "Rivista di diritto bancario", 2021, n. 1

G. Olivieri (2021), *PSD2 e tutela della concorrenza nei nuovi mercati dei servizi di pagamento digitali*, in "Giurisprudenza commerciale", 2021, n. 3

C. Parodi (1997), *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in "Diritto penale processuale", 1997

G. Pascuzzi (2020), *Il diritto dell'era digitale*, il Mulino, 2020

C. Pecorella (2012), *Truffe on-line: momento consumativo e competenza territoriale*, in "Rivista italiana diritto e procedura penale", 2012, n. 1

S. Piancastelli (2015), *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in "Diritto Penale Contemporaneo", 3 marzo 2015

Polizia postale (2023), *Resoconto attività 2022 della polizia postale e delle comunicazioni e dei centri operativi sicurezza cibernetica*, 3 gennaio 2023

E. Reccia (2022), *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in "Archivio Penale", 2022, n. 2

C. Sarzana (2010), *Informatica, internet e diritto penale*, Giuffrè, 2010

S. Sica, B.M. Sabatino (2021), *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, in "Diritto dell'informazione e dell'informatica", 2021, n. 1

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0117 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Mauro Barberio

L'uso dell'intelligenza artificiale nell'art. 30 del d.lgs. 36/2023 alla prova dell'AI Act dell'Unione europea*

Il presente lavoro, in prossimità della pubblicazione dell'AI Act dell'Unione europea, mette in relazione l'innovativa (per il sistema giuridico italiano) applicazione dell'intelligenza artificiale al campo dei pubblici appalti – così come dispone l'art. 30 del d.lgs. 36/2023 – con gli istituti di matrice eurounitaria che stanno per vedere la luce. Effettuata una breve introduzione sui sistemi di intelligenza artificiale utilizzabili nel settore in esame, lo scritto si sofferma, *in primis,* sulla problematica qualificazione dell'ambito dei pubblici appalti come attività ad alto rischio, ai sensi e per gli effetti dell'Allegato III dell'AI Act. Viene, altresì, messo in evidenza su chi debba gravare, e da chi debba provenire, quel "contributo umano" che l'art. 30 del d.lgs. 36/2023 stabilisce come inderogabile ai fini della legittimità dei provvedimenti automatizzati nel settore dei pubblici appalti e le ripercussioni che determina, in tal senso, l'individuazione dell'"operatore", pubblico e privato, quale figura chiave e giuridicamente responsabile della sorveglianza umana. Il lavoro si chiude soffermandosi sui sistemi di governance e di prevenzione dei rischi, così come impostati dal legislatore europeo, con particolare riferimento agli istituti di cui alla valutazione d'impatto e alla sperimentazione normativa.

Intelligenza artificiale – Appalti pubblici – Controllo umano – Governance e sperimentazione normativa

The Use of artificial intelligence in Article 30 of Legislative Decree 36/2023 to the test of the EU AI Act

The present work, in close to the publication of the AI Act of the European Union, relates the innovative (for the Italian legal system) application of artificial intelligence to the field of public procurement – as provided for in Article 30 of Legislative Decree 36/2023 – with the EU institutions that are about to see the light of day. With a brief introduction to the artificial intelligence systems that can be used in the sector in question, the paper focuses, first of all, on the problematic qualification of the field of public procurement as a high-risk activity, pursuant to and for the effects of Annex III of the AI Act. It is also highlighted who should burden, and from whom should come, that 'human contribution' that Article 30 of Legislative Decree 36/2023 establishes as mandatory for the purposes of the legitimacy of automated measures in the field of public procurement and the repercussions that determine, in this sense, the identification of the 'operator', public and private, as a key figure and legally responsible for human surveillance. The work ends by focusing on the governance and risk prevention systems, as set by the European legislator, with particular reference to impact assessment and regulatory testing.

Artificial intelligence – Public procurement – Human control – Governance and regulatory testing

L'Autore è avvocato amministrativista abilitato presso le magistrature superiori

* Relazione tenuta al Convegno di studi presso l'Università degli Studi di Cagliari "L'intelligenza artificiale nel diritto amministrativo", 27 ottobre 2023.

1. L'art. 30 del Codice dei contratti pubblici e l'automazione delle attività amministrative

L'art. 30 del nuovo Codice dei contratti rappresenta una novità assoluta nello scenario normativo nazionale in quanto, come noto, ha introdotto e incentivato l'automazione delle attività amministrative nel ciclo di vita dei contratti pubblici, quindi dalla programmazione sino alla fase di esecuzione.

Contestualmente il legislatore ha cercato di calibrare alcuni contrappesi miranti, principalmente, a far sì che le logiche di funzionamento delle soluzioni tecnologiche prescelte potessero essere, non solo, adeguatamente comprese e accessibili, ma anche non esclusivamente riferibili alla macchina. Imponendo che la decisione algoritmica, all'interno del processo decisionale, possa, quindi, essere controllata, validata o smentita dal controllo(re) umano, anche attraverso l'adozione di «ogni misura tecnica e organizzativa atta a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori».

Uno dei primi problemi da porsi, almeno così sembra a chi scrive, è quello teso all'individuazione dell'ambito entro cui, relativamente agli appalti pubblici, potrebbe risultare più funzionale e aderente l'uso dell'intelligenza artificiale. La risposta non risulta particolarmente complicata: si tratta, in tutta evidenza, della fase istruttoria e, quindi, in modo precipuo, della fase di valutazione delle offerte e, precisamente, di quelle tecniche. In quanto le offerte economiche sono già da tempo oggetto di formule (in verità piuttosto essenziali) alfa numeriche che non necessitano dell'intelligenza artificiale per essere sviluppate e controllate.

Non sembra, in effetti, esservi altro ambito, all'interno del procedimento di gara (se non forse quello legato all'eventuale fase di verifica dell'anomalia), maggiormente dedicato per l'applicazione dell'intelligenza artificiale

Dati i presupposti della disposizione codicistica, e ferme le prime analisi effettuate dalla dottrina in merito agli aspetti chiaroscurali della predetta disciplina normativa[1], risulta, in questa sede, di peculiare interesse comprendere quali possano essere le relazioni intercorrenti tra l'art. 30

1. Cfr. Gallone 2023 e, sia consentito, Barberio 2023. Cfr. anche Simoncini 2019; Amato Mangiameli 2022; Taddei Elmi 2021.

del d.lgs. 31 marzo 2023, n. 36 e il nuovo regolamento eurounitario, AI Act (che risulta in fase di approvazione[2]).

Definite le fasi procedimentali di carattere valutativo-decisionale, votate, precipuamente, all'uso dell'intelligenza artificiale, diviene conseguente comprendere quale specifica tipologia di IA possa essere maggiormente aderente alle necessità delle stazioni appaltanti. Tutto ciò anche a voler tralasciare l'aspetto – tutt'altro che irrilevante o, ancor meno, scontato ma non decisivo nella presente analisi – se si possa, o meno, procedere, mediante i provvedimenti automatizzati, a effettuare scelte discrezionali o se questi debbano essere, esclusivamente, destinati per dinamiche procedimentali vincolate[3].

Lo strumento automatizzato più funzionale per un'eventuale comparazione delle offerte tecniche è certamente quello proprio delle tecnologie di cui ai modelli linguistici di grandi dimensioni (tradotto dall'acronimo LLMs – *Large Language Models*), cui appartengono quei sistemi che si basano su degli *input* sorgenti (prompt) che poi, conseguentemente, generano e restituiscono una sequenza di parole, codici o dati (output). I sistemi più recenti di LLMs includono GPT-3, PaLM, LaMDA, Gopher and OPT[4].

Questi modelli hanno una capacità straordinaria di rispondere alle sollecitazioni che vengono loro proposte – tanto con riferimento alla qualità del riscontro quanto all'immediatezza della risposta – ma, per poter essere adeguatamente consultati e ottenere esiti conferenti ed efficaci, necessitano di due indefettibili presupposti che ne rendano sostenibili gli esiti (output, ossia "previsioni, raccomandazioni o decisioni che rispondono agli obbiettivi del sistema sulla base degli input provenienti da tale ambiente") o che ne possano consentire, altrimenti, il loro rigetto attraverso un'istruttoria che possa portare alla loro smentita[5].

2. La disciplina eurounitaria tra *data training* e governance

I due presupposti per una corretta ed efficace applicabilità alle regole dell'evidenza pubblica delle dinamiche proprie dei LLMs si fondano, da un lato, su un sistema di addestramento (training) che dovrà essere adeguato alla specifica attività istruttoria che verrà effettuata. D'altro lato sarà necessario impostare e garantire un rigoroso sistema di controlli (governance) da porre in essere tanto a posteriori quanto, però, anche a priori[6], al fine di controllare, verificare ed, eventualmente, smentire la decisione automatizzata.

Con riferimento al primo problema e alla necessità di un adeguato addestramento del sistema di intelligenza artificiale, non sembra inutilmente ozioso far rilevare come i predetti sistemi LLMs rispondono alle sollecitazioni proposte (tramite

2. «The Council agreed the EU Member States' general position in December 2021. Parliament voted on its position in June 2023. EU lawmakers are now starting negotiations to finalise the new legislation, with substantial amendments to the Commission's proposal including revising the definition of AI systems, broadening the list of prohibited AI systems, and imposing obligations on general purpose AI and generative AI models such as ChatGPT», European Parliament (*Artificial Intelligence Act*).
3. Lo scontro interpretativo, in merito a questa problematica, è già in essere all'interno della giustizia amministrativa tra le sentenze n. 2270, sez. VI, dell'8 aprile 2019 («la discrezionalità amministrativa …non può essere demandata al software, è quindi da rintracciarsi al momento dell'elaborazione dello strumento digitale») e n. 8472, sez. VI, del 13 dicembre 2019 che, invece, facendo leva su una, per la verità discutibile, contestazione «a monte dell'attualità di una tale distinzione» (tra attività amministrativa vincolata piuttosto che discrezionale, n.d.a.), ammette che «se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità».
4. Mokander-Schuett-Kirk-Floridi 2023; Floridi-Chiriatti 2020; Charlotin 2023.
5. Art. 30 co. 3 lett. b «non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata».
6. Una corretta governance dovrebbe occuparsi, con particolare attenzione, anche della fase anteriore non tanto e non solo per la verifica dell'addestramento della macchina (training) ma anche per prevenire distorsioni ed errori assieme alla chiara definizione delle regole e modalità di interventi correttivi.

input) tanto proattivamente quanto più hanno sviluppato, mediante adeguato training, le proprie conoscenze e abilità all'interno di sistemi adeguati di apprendimento automatico (*machine learning*), anche attraverso un sistema di apprendimento profondo (*deep learning*) tramite reti neurali.

È agevolmente rilevabile (e di questo si dovrà, necessariamente, tenere conto), infatti, come i sistemi di IA abbiano possibilità di funzionamento attraverso «livelli di autonomia variabili, il che significa che dispongono almeno di un certo grado di autonomia di azione rispetto ai controlli umani e di capacità di funzionare senza l'intervento umano» (considerando n. 6 AI Act dell'Ue). Quel grado di autonomia variabile, che può arrivare a essere anche assoluto, si sviluppa, però, all'interno di un ambiente (che è il contesto entro cui operano i sistemi automatizzati) che è condizionato dagli input forniti, da ciò che è già ivi presente e, poi, successivamente, lo sarà pure dagli stessi output creati dal sistema che, quindi, lo implementano e alimentano («Tale output influenza ulteriormente detto ambiente anche solo mediante l'introduzione di nuove informazioni» – cons. n. 6). In questi termini appare evidente che gli esiti che vengono sollecitati al sistema di intelligenza artificiale sono condizionati grandemente dall'ambiente entro cui il medesimo pasce e si nutre.

La prima sfida, pertanto – anche a livello di governance "preventiva" – sarà quella di garantire (e verificare) che il sistema si sia sviluppato in un ambiente adeguato con riferimento al preteso risultato da raggiungere. Ambiente di addestramento del sistema automatizzato che, evidentemente, condizionerà il livello qualitativo dell'esito atteso. Appare pertinente far rilevare, infatti, come (anche in termini di prevenzione di eventuali risposte discriminatorie o per evitare la decantazione di *bias*) la criticità si ravvisi e si possa sviluppare, non tanto e non solo, nella tipologia di algoritmo utilizzato, quanto piuttosto nell'ambiente e nei dati (*data training*) attraverso i quali il sistema è stato, o si è, autonomamente, addestrato.

Se non vi saranno set di dati adeguati, qualitativamente e quantitativamente, il risultato che la macchina restituirà sarà parziale, limitato, errato o qualitativamente insufficiente.

Il legislatore eurounitario ha chiara questa problematica e la espone, in maniera efficacissima, nei considerando nn. 42, 43 e 44 («Un accesso ai dati di alta qualità svolge un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessaria l'attuazione di adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento e, ove applicabile, di convalida e prova, incluse le etichette, dovrebbero essere sufficientemente pertinenti, rappresentativi, adeguatamente verificati in termini di errori e il più possibile completi alla luce della finalità prevista del sistema. Dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato, prestando particolare attenzione all'attenuazione di possibili distorsioni nei set di dati, che potrebbero comportare rischi per i diritti fondamentali o risultati discriminatori per le persone interessate dal sistema di IA ad alto rischio. Le distorsioni possono ad esempio essere intrinseche agli insiemi di dati di base, specie se si utilizzano dati storici, inseriti dagli sviluppatori degli algoritmi o generati quando i sistemi sono attuati in contesti reali. I risultati forniti dai sistemi di IA sono influenzati da tali distorsioni intrinseche, che sono destinate ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti … I requisiti relativi alla governance dei dati possono essere soddisfatti ricorrendo a terzi che offrono servizi di conformità certificati, compresa la verifica della governance dei dati, dell'integrità dei set di dati e delle pratiche di addestramento, convalida e prova dei dati»).

Dovrebbe, quindi, essere garantito (anche a livello di specifiche tecniche di cui all'art. 79 e all'All. II.5 del d.lgs. 36/2023) – prima di essere utilizzato in determinate gare e per valutare le conseguenti offerte tecniche – che il sistema di intelligenza artificiale sia certificato per aver operato all'interno di specifici ambienti e con set di dati pertinenti e adeguatamente rappresentativi. Non può che essere questo il senso di quanto dispone l'art. 16.1 a-*quater* dell'AI Act che impone, per i sistemi di IA ad alto rischio, che siano fornite «le specifiche per i dati di input o qualsiasi altra informazione

pertinente in termini di set di dati utilizzati, compresi i relativi limiti e le relative ipotesi, tenendo conto della finalità prevista e degli usi impropri prevedibili e ragionevolmente prevedibili del sistema di IA».

3. Tra apprendimento supervisionato e *deep learning*

Alla luce di queste prime, essenzialissime, considerazioni sembra potersi affermare come, all'interno del quadro stabilito dall'art. 30 del Codice dei contratti pubblici, il più sicuro e affidabile sistema di intelligenza artificiale, per quanto quivi di interesse, risulti essere quello con apprendimento supervisionato. In quanto si manifesta come lo strumento che può rispondere, in maniera più efficace, alle condizioni ivi stabilite dal legislatore che, non a caso, impone una supervisione effettiva, attraverso un efficace contributo umano che possa essere "capace di controllare, validare ovvero smentire la decisione automatizzata". Sistema che, peraltro, quando non li elimina, riduce notevolmente output complessi e opachi che ne rendono difficile la comprensibilità e, quindi, anche la possibilità di esplicazione degli esiti[7]. Il legislatore europeo ha ben chiaro il rischio della predetta deriva e, infatti, per quelle attività c.d. "ad alto rischio"[8] impone, all'art. 14.1, sistemi di intelligenza artificiale con apprendimento supervisionato: «I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da essere efficacemente supervisionati da persone fisiche in misura proporzionale ai rischi associati a tali sistemi».

Viene, insomma, sostanzialmente, posto il veto – per le attività ad alto rischio – per quei sistemi di intelligenza artificiale con capacità di apprendimento profondo (c.d *deep learning*) senza supporto umano. Questa modalità di apprendimento, infatti, non prevede alcun intervento umano che possa suggerire le risposte possibili o intervenire in via diretta, in quanto «deve essere messa in condizione di sbagliare un numero così elevato di

7. AI Act, considerando 6-*bis:* «La funzione e gli output di molti di questi sistemi di IA si basano su relazioni matematiche astratte che per gli esseri umani risultano difficili da comprendere e monitorare e i cui input specifici sono difficili da rintracciare. Tali caratteristiche complesse e opache (elemento "scatola nera") incidono sulla rendicontabilità e sulla spiegabilità».

8. AI Act, art. 6 – *Regole di classificazione per i sistemi di IA ad alto rischio*: «A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza ai sensi della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi in relazione ai rischi per la salute e la sicurezza ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II. 2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio i sistemi di IA che rientrano in uno o più settori critici e casi d'uso di cui all'allegato III, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche. Qualora un sistema di IA rientri nell'allegato III, punto 2, è considerato ad alto rischio se presenta un rischio significativo di danno per l'ambiente. Sei mesi prima dell'entrata in vigore del presente regolamento, la Commissione, previa consultazione dell'ufficio per l'IA e dei pertinenti portatori di interessi, fornisce orientamenti che specificano chiaramente le circostanze in cui l'output dei sistemi di IA di cui all'allegato III comporterebbe un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche o i casi in cui non lo farebbe». Per l'All. III: «I sistemi di IA di cui ai punti da 1 a 8-*bis* rappresentano casi d'uso critici e sono tutti considerati sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, a condizione che soddisfino i criteri di cui a tale articolo: 1) Sistemi biometrici e basati su elementi biometrici. …2. Gestione e funzionamento delle infrastrutture critiche. …3. Istruzione e formazione professionale. …4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo. …5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi. …6. Attività di contrasto. …7. Gestione della migrazione, dell'asilo e del controllo delle frontiere. …8. Amministrazione della giustizia e processi democratici»; Mollicone 2023.

volte da individuare l'errore e provvedere in autonomia a correggere la propria sequenza»[9].

4. Attività ad alto rischio e appalti pubblici: quale relazione

La domanda è, a questo punto, obbligata: il settore dei pubblici appalti rientra o meno all'interno delle attività ad alto rischio?

La risposta a questo interrogativo dovrebbe essere verosimilmente negativa qualora ci si fermasse all'analisi specifica del settore e, quindi, sulla base di una verifica strutturale della disposizione normativa. Giusto quanto fa rilevare l'AI Act (all'art. 6 e nell'Allegato III), gli appalti pubblici non sono, infatti, qualificabili *ex se* come un ambito predicabile quale settore ad alto rischio.

A fronte, però, di una verifica sostanziale e in concreto, dell'operato che la stazione appaltante porrà effettivamente in essere, non sarebbe agevole riuscire ad estromettere la singola procedura di gara da una possibile classificazione come attività qualificabile ad alto rischio. Tanto nel caso in cui l'appalto dovesse ricadere, specificamente, in uno di quegli ambiti predeterminati dal legislatore eurounitario come settore ad alto rischio, in forza di una correlazione che non sembra possa essere troppo rarefatta (basti pensare agli ambiti della "gestione e funzionamento delle infrastrutture critiche", dell'"accesso a prestazioni e servizi pubblici e a servizi privati essenziali" o della "gestione e funzionamento della fornitura di acqua, gas, riscaldamento, energia elettrica e infrastrutture digitali critiche"). Così come non sembra potersi escludere, in termini più generali, come ad alto rischio quell'attività valutativa intrinseca, sui fatti e/o disposizioni normative, qualora effettuata da un'amministrazione, o da un organo amministrativo, attraverso sistemi di intelligenza artificiale[10].

Restano, comunque, da considerare due aspetti, sui quali è necessario, seppur *en passant*, porre l'accento, in merito alla sufficienza e rilevanza del concetto di alto rischio in materia di pubblici contratti. Da un lato appare illusorio pretendere di incasellare, in modo determinato e preventivo, la fenomenologia di tutti rischi – non solo futuri, ma pure quelli presenti, alti o bassi che possano essere ritenuti – e i loro correlativi ambiti, a fronte dell'imprevedibilità e liquidità della materia[11]. D'altro canto chi scrive aderisce a quella tesi che

9. Pesucci 2022; cfr. ancora Lo Sapio 2021: «I sistemi di Deep Learning utilizzano un'architettura di modelli matematici ispirata alle reti neurali biologiche: le cd. reti neurali artificiali. Tale modello è costituito da un gruppo di interconnessioni di informazioni (si parla infatti di approccio di "connessionismo" al calcolo, contrapposto all'approccio simbolista): gli input trasmettono i segnali, ad una potenza ovviamente incomparabile con quella dei neuroni biologici, ai diversi nodi che costituiscono una rete complessa (deep) e nel corso dell'apprendimento, i "pesi" di ciascun nodo vengono continuamente riparametrati, in un percorso non lineare e multistrato la cui ricostruzione però sfugge alla comprensione umana».

10. Il considerando 40 recita, in modo non inequivocabile, «È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o da un organo amministrativo, o per loro conto, per assistere le autorità giudiziarie o gli organi amministrativi nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie» e, pure, l'Allegato III, punto 8, lett. a, fa rilevare come siano ad alto rischio: «i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o da un organo amministrativo, o per loro conto, per assistere un'autorità giudiziaria o un organo amministrativo nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie».

11. «AI harms are very different in different contexts, where they might be already addressed by particular sectoral laws. At the same time, most AI harms can readily be traced to a pattern of similar problems. Problems of incomplete or biased training data ("garbage in, garbage out") and poorly designed human machine systems (including ignoring known cognitive biases and overreliance on a human in the loop) resonate across sectors», Kaminski 2022. «Moreover, given the multiplicity and complexity of the ethical and social risks associated with LLMs, we anticipate that policy responses will need to be multifaceted and incorporate several complementary governance mechanisms. As of now, technology providers and policymakers have only started experimenting with different governance mechanisms, and how LLMs should be governed remains an open question», Mokander-Schuett-Kirk-Floridi 2023; Engler 2023.

qualifica, di per sé stesse, rischiose – non tanto l'ambito di utilizzazione quanto piuttosto – l'applicazione e l'utilizzazione concrete dei sistemi generativi di intelligenza artificiale[12].

Ferme le predette valutazioni, il primo presupposto per un'adeguata e legittima utilizzazione dell'intelligenza artificiale, nei procedimenti di gara, sarà quello di avere un sistema supervisionato che sia stato addestrato in un ambiente adeguato affinché possa restituire output che siano i più conferenti, logici e corretti possibili e che possano essere controllati, verificati e, nell'eventualità, anche smentiti da un sorvegliante umano che disponga di «un livello sufficiente di alfabetizzazione in materia di IA conformemente all'articolo 4-*ter* nonché del sostegno e dell'autorità necessari per esercitare tale funzione, durante il periodo in cui il sistema di IA è in uso e per consentire indagini approfondite a seguito di un incidente» (art. 14.1 AI Act).

5. Contributo umano e responsabilità dell'"operatore" privato e pubblico

La declinazione necessitata di questo, primo, presupposto ci conduce all'interrogativo in ordine a quale debba essere il contributo umano preteso per giungere, eventualmente, anche alla smentita della decisione automatizzata, ai sensi della lett. b) del co. 3 dell'art. 30 del Codice dei contratti pubblici che, come noto, impone la non esclusività della decisione algoritmica.

L'intero AI Act dell'Ue è, peraltro, pervaso dalla necessità dell'intervento umano o, meglio, della "sorveglianza umana"[13], finalizzata a evitare e correggere le, sempre, possibili distorsioni sistemiche e per far sì che vengano «adottate misure tecniche e organizzative per garantire che i sistemi di IA ad alto rischio siano quanto più possibile resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi» (art. 15.3 AI Act).

La cattiva notizia – se così la si può definire – che determinerà, a parere di chi scrive, la fuga delle stazioni appaltanti dall'auspicato (da parte del legislatore del d.lgs. 36/2023) uso delle procedure automatizzate, trae la propria ragion d'essere dal tarlo che si insinua in conseguenza del considerando n. 58-*bis* che responsabilizza, in maniera massiva, gli "operatori"[14], i quali, ai sensi dell'art. 3.4, vengono individuati in

12. «The alternative scenario would be that all generative AI systems would fall under the high risk category because it cannot be excluded that they may be used also in a high-risk area. In that case, there may be a serious risk of over-regulation. For this reason, rather than trying to fit general-purpose AI systems into existing high-risk categories, we propose that they should be considered a general-risk category in their own right, similar to the way that chatbots and deep fakes are considered a separate risk category of their own, and subject to legal obligations and requirements that fit their characteristics», Helberger-Diakopoulos 2023.

13. Cfr. considerando nn. 1, 4-*bis*, 9-*bis*, 43 e l'art. 4-*bis*. Tra gli altri si segnalano poi gli artt. 7 e 14 anche se, in effetti, il richiamo alla possibilità di «di intervenire sul funzionamento del sistema di IA ad alto rischio o di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga, che consenta di arrestare il sistema in condizioni di sicurezza» appare piuttosto *naif*.

14. Considerando 58-*bis*: «Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche dal modo in cui tali sistemi di IA sono utilizzati. Gli operatori di sistemi di IA ad alto rischio svolgono pertanto un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA. Gli operatori sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi emarginati e vulnerabili. Gli operatori dovrebbero individuare strutture di governance adeguate in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana, le procedure di gestione dei reclami e le procedure di ricorso, dal momento che le scelte relative alle strutture di governance possono essere determinanti per attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Al fine di garantire in maniera efficiente la tutela dei diritti fondamentali, l'operatore di sistemi di IA ad alto rischio dovrebbe quindi effettuare una valutazione d'impatto sui diritti fondamentali prima di metterli in servizio. La valutazione d'impatto dovrebbe essere corredata di un piano dettagliato che descriva le misure o gli strumenti che contribu-

«qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

Il pericolo dell'intelligenza artificiale viene, quindi, normativamente collegato non tanto alla sua materiale produzione e messa in commercio, bensì, massimamente, al suo concreto utilizzo. Il rischio viene riconnesso all'immanenza del suo uso e, pertanto, viene scaricato sull'operatore che viene individuato come responsabile e come destinatario di una notevole messe di obblighi[15], tra i quali, per quanto in questa sede rileva, brilla il dovere di sovrintendenza umana sulle attività automatizzate («Nella misura in cui esercitano un controllo sul sistema di IA ad alto rischio, gli operatori: i) attuano la sorveglianza umana conformemente ai requisiti stabiliti nel presente regolamento; ii) garantiscono che le persone fisiche preposte ad assicurare la sorveglianza umana dei sistemi di IA ad alto rischio siano competenti, adeguatamente qualificate e formate e dispongano delle risorse necessarie per assicurare l'efficace supervisione del sistema di IA a norma dell'articolo 14; iii) garantiscono che le misure pertinenti e adeguate in materia di robustezza e cibersicurezza siano periodicamente monitorate per verificarne l'efficacia e siano periodicamente adeguate o aggiornate» – art. 29.1-*bis*).

Ulteriore interrogativo è quello di stabilire se la sorveglianza umana, il controllo umano o la riserva di umanità, comunque la si voglia definire, sia derogabile o, meglio, se sia giuridicamente disponibile da parte del privato, eventualmente sollecitato in merito da un'amministrazione che intenda procedere, per esempio, attraverso sistemi di intelligenza artificiale non supervisionati e, quindi, non governati da successiva sorveglianza umana. Se vi sia, insomma, la possibilità di prestare consenso a un'attività esclusivamente automatizzata senza possibilità che venga controllata, validata o smentita. In termini generali, dal lato squisitamente normativo, in forza del regolamento Ue 679/2016 – richiamato copiosamente dall'AI Act e ritenuto trasversalmente applicabile alla disciplina *de qua* – nulla sembra ostarvi. Il citato regolamento ammette, infatti, espressamente la disponibilità del consenso, in siffatte ipotesi, ai sensi dell'art. 22: «1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: …c) si basi sul consenso esplicito dell'interessato»[16].

iranno ad attenuare i rischi per i diritti fondamentali individuati al più tardi a partire dal momento della loro messa in servizio. Se tale piano non può essere individuato, l'operatore dovrebbe astenersi dal mettere in servizio il sistema. Nell'effettuare tale valutazione d'impatto, l'operatore dovrebbe informare l'autorità nazionale di controllo e, nella misura più ampia possibile, i pertinenti portatori di interessi nonché i rappresentanti dei gruppi di persone che potrebbero essere interessati dal sistema di IA al fine di raccogliere le informazioni pertinenti ritenute necessarie per effettuare la valutazione d'impatto e sono incoraggiati a rendere pubblica la sintesi della loro valutazione d'impatto sui diritti fondamentali sul loro sito web online. Tali obblighi non dovrebbero applicarsi alle PMI che, data la mancanza di risorse, potrebbero incontrare difficoltà nello svolgimento di tale consultazione. Tuttavia, esse dovrebbero altresì adoperarsi per coinvolgere tali rappresentanti nello svolgimento della loro valutazione d'impatto sui diritti fondamentali. Inoltre, dati il potenziale impatto e la necessità di sorveglianza e controllo democratici, gli operatori di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione, nonché gli operatori che sono imprese designate come gatekeeper a norma del regolamento (UE) 2022/1925, dovrebbero essere tenuti a registrare l'uso di qualsiasi sistema di IA ad alto rischio in una banca dati pubblica. La registrazione è possibile, su base volontaria, anche per altri operatori».

15. Cfr. artt. 23, 27, 28, 29, 51, 62.

16. «Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito"» – Garante della privacy, "Principi fondamentali del trattamento". Si richiama, però, una recente sentenza della Corte di cassazione che prescrive un percorso, per il rilascio del consenso, più articolato a garanzia del privato: «Il problema, per la liceità del trattamento, era invece (ed è) costituito dalla validità – per l'appunto – del consenso che si assume prestato al momento dell'adesione. E non può logicamente affermarsi che l'adesione a una piattaforma da parte

La ricaduta pratica del consenso all'eventuale disumanizzazione del procedimento (e quindi del conseguente provvedimento) automatizzato non potrebbe mai essere la, ipoteticamente, sperata emarginazione e deresponsabilizzazione dell'umano, in quanto il nostro sistema costituzionale impone che sia l'uomo e non la macchina a rispondere delle proprie azioni[17].

6. La valutazione d'impatto come strumento principale di governance e suoi limiti

Un adeguato sistema di governance rappresenta il secondo pilastro per la migliore, e legittima, utilizzazione, nel campo dei pubblici appalti (ma non solo, ovviamente), dei sistemi di intelligenza artificiale.

Nonostante vi sia chi propone sistemi di governance complessi e differentemente articolati[18], chi scrive ritiene di aderire all'impostazione fornita da alcuni studiosi statunitensi che hanno evidenziato la specificità e l'assoluta novità della sfida lanciata dall'intelligenza artificiale che impone risposte totalmente nuove e altre[19] rispetto a una concezione, di controllo e verifica, che potrebbe essere definita tradizionale.

La legislazione europea sta sviluppando il proprio indirizzo sulla governance cercando di trovare delle linee di azione innovative e coraggiose sulle quali – in un quadro liquido quale quello in esame – saranno il tempo e l'esperienza a darci risposte in merito alla loro efficacia e, quindi, alla necessità di eventuali, quanto probabili, correzioni.

Così come la responsabilità, anche la gestione della governance, viene delegata agli operatori che, ai sensi del considerando 58-*bis*, dovrebbero «individuare strutture di governance adeguate in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana, le procedure di gestione dei reclami e le procedure di ricorso, dal momento che le scelte relative alle strutture di governance possono essere determinanti per attenuare i rischi per i diritti fondamentali in casi d'uso concreti») e determinare – a priori e qualora si rientri «in uno o più settori critici e casi d'uso di cui all'Allegato III» (ved. art. 6.2 AI Act) – una modalità preventiva di valutazione tesa a qualificare/quantificare l'impatto del sistema di intelligenza artificiale, redigendo un "piano dettagliato" che descriva, tra l'altro, le misure e gli strumenti finalizzati all'attenuazione dei rischi e che raccolga le informazioni pertinenti ritenute necessarie per effettuare l'indicata valutazione.

Il predetto istituto (*rectius* la valutazione di impatto[20]) conosce in ambito europeo la propria

dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi riconoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati», Corte di cassazione, sez. I civ, n. 14381 del 25 maggio 2021.

17. «La mancanza di effettivo contributo umano determinerebbe evidenti questioni di legittimità costituzionale in relazione alla violazione degli artt. 28, 97 co. 3 e 98 che valorizzano le funzioni e le responsabilità dei pubblici dipendenti o in relazione alla violazione dell'art. 54 co. 2 che riconnette le funzioni pubbliche alla persona fisica (anche perché sulla base delle, tuttora insuperate, leggi di Isaac Asimov sulla robotica, il robot non può essere chiamato a responsabilità)» Barberio 2023; Gallone 2023.

18. «Our findings most directly concern technology providers as they are primarily responsible for ensuring that LLMs are legal, ethical, and technically robust. Such providers have moral and material reasons to subject themselves to independent audits, including the need to manage financial and legal risks and build an attractive brand». Si tratta di un approccio innovativo quanto distonico rispetto a quello eurounitario che responsabilizza, non tanto i fornitori o i produttori quanto, come sopra fatto rilevare, massimamente, gli operatori. Mokander-Schuett-Kirk-Floridi 2023.

19. «AI cannot be governed like any previous technology, and it is already shifting traditional notions of geopolitical power … the challenge is clear: to design a new governance framework fit for this unique technology. If global governance of IA is to become possible, the international system must move past traditional conceptions of sovereignty and welcome technology companies to the table». Bremmer-Suleyman 2023.

20. Art. 29-*bis* AI Act: «Prima di mettere in servizio un sistema di IA ad alto rischio quale definito all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA destinati ad essere utilizzati nel settore 2 dell'allegato III, gli operatori effettuano una valutazione dell'impatto dei sistemi nel contesto specifico di impiego …».

applicazione in settori particolarmente sensibili quali quello ambientale[21] e quello della tutela dei dati personali[22]. La valutazione di impatto è stata pensata, anche all'interno dell'AI Act, quale strumento necessario per la regolazione specifica dell'intelligenza artificiale nelle ipotesi ad alto rischio e per minimizzarne gli effetti e le possibili ricadute negative.

Si tratta di un sistema di governance teso a individuare, preventivamente, i rischi e a descrivere le misure e gli strumenti finalizzati alla riduzione, ove possibile, di ogni eventuale conseguenza negativa cagionabile dal sistema di IA. Qualora, peraltro, per qualche ragione, non dovesse essere possibile redigere un piano dettagliato ai sensi dell'art. 29-*bis*: «l'operatore si astiene dal mettere in servizio il sistema di IA ad alto rischio e informa senza indebito ritardo il fornitore e l'autorità nazionale di controllo. Le autorità nazionali di controllo, a norma degli articoli 65 e 67, tengono conto di tali informazioni quando conducono indagini sui sistemi che presentano un rischio a livello nazionale».

Il legislatore eurounitario indica quei contenuti generali che la valutazione di impatto deve, necessariamente, contenere, ai sensi dell'art. 29-*bis* dell'AI Act, ossia: «a) una chiara descrizione della finalità prevista per la quale verrà utilizzato il sistema; b) una chiara descrizione dell'ambito geografico e temporale previsto per l'uso del sistema; c) le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema; d) la verifica che l'uso del sistema è conforme al diritto dell'Unione e nazionale in materia di diritti fondamentali; e) l'impatto ragionevolmente prevedibile sui diritti fondamentali di mettere in servizio il sistema di IA ad alto rischio; f) determinati rischi di danno suscettibili di incidere sulle persone emarginate e sui gruppi vulnerabili; g) l'impatto negativo ragionevolmente prevedibile dell'utilizzo del sistema sull'ambiente; h) un piano dettagliato su come saranno attenuati i danni o l'impatto negativo sui diritti fondamentali individuati; j) il sistema di governance che sarà messo in atto dall'operatore, compresa la supervisione umana, la gestione dei reclami e i mezzi di soccorso».

La critica che si ritiene di muovere alla disciplina normativa testé richiamata va individuata nel fatto che la stessa si concentra, quasi totalmente, sul rischio di derive discriminatorie e violazioni di diritti individuali, ma non sembra curarsi a sufficienza della restituzione (negli ambiti pubblicistici e istituzionali) di dati erronei, imprecisi o parziali. Si ritiene, pertanto, che, nella misura in cui un sistema di IA intervenga in una procedura di affidamento, qualificabile come ad alto rischio, alla luce della clausola residuale di cui all'art. 29-*bis* («Tale valutazione comprende, *almeno*[23], i seguenti elementi»), la valutazione di impatto possa essere adeguatamente implementata dall'operatore, in sede di analisi dei possibili e specifici impatti, con contenuti ulteriori e atipici tesi alla migliore efficacia e calibrazione del sistema di intelligenza artificiale.

7. La sperimentazione normativa: un'occasione da non perdere

Una novità che potrebbe risultare utilissima (per sviluppare analisi e dinamiche innovative, di carattere sperimentale, anche nell'ambito dei pubblici appalti e, comunque, dei procedimenti amministrativi) è quella che, ai sensi dell'art. 53 dell'AI Act, consente degli spazi di sperimentazione normativa per l'IA («1. Gli Stati membri istituiscono almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in applicazione del presente regolamento. Tale spazio di sperimentazione può anche essere istituito congiuntamente con uno o diversi altri Stati membri. 1-*bis*. Possono essere istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale o congiuntamente con altri Stati membri … 1-*quater*. Le autorità costituenti assegnano risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva. 1 quinquies. Gli spazi di sperimentazione normativa per l'IA, conformemente ai criteri di cui all'articolo 53-*bis*, garantiscono un ambiente controllato che promuove l'innovazione e facilita

21. Direttiva 85/337/CEE del 27 giugno 1985.

22. Art. 35 del regolamento Ue 2016/679 del 27 aprile 2016.

23. Corsivo aggiunto.

lo sviluppo, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico concordato tra i potenziali fornitori e l'autorità costituente; 1-*sexies*. L'istituzione di spazi di sperimentazione normativa per l'IA è intesa a contribuire ai seguenti obiettivi: a) le autorità competenti forniscano orientamenti ai potenziali fornitori di sistemi di IA per conseguire la conformità normativa con il presente regolamento o, se del caso, ad altre pertinenti normative applicabili dell'Unione e degli Stati membri; b) i potenziali fornitori consentano e agevolino la sperimentazione e lo sviluppo di soluzioni innovative relative ai sistemi di IA; c) apprendimento normativo in un ambiente controllato».

Si tratta di un'occasione irripetibile che il legislatore nazionale (così come per quelli regionali più dinamici e propositivi) non dovrebbe perdere e attivare ben prima dell'entrata in vigore del regolamento comunitario[24] per portarsi avanti nell'applicazione pratica e sperimentale dell'intelligenza artificiale nella sua relazione con l'amministrazione pubblica. Questa concessione normativa consente di calibrare, anche per "lotti" o "stati di avanzamento", l'efficacia dell'intelligenza artificiale in ambiti specifici e di testarne l'efficacia, senza la pretesa di definire, da subito, un sistema normativo compiuto che rischierebbe di essere o troppo acerbo o, altrimenti, di nascere già superato.

Quale migliore applicazione, per la sperimentazione normativa, potrebbe esserci rispetto a quella degli appalti pubblici che hanno già la porta spalancata, all'utilizzazione dell'intelligenza artificiale, dall'art. 30 del d.lgs. 36/2023?

Riferimenti bibliografici

A.C. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

M. Barberio (2023), *L'utilizzo degli algoritmi e l'intelligenza artificiale tra futuro prossimo e incertezza applicativa*, giugno 2023

I. Bremmer, M. Suleyman (2023), *The AI Power Paradox. Can States Learn to Govern Artificial Intelligence — Before It's Too Late?*, in "Foreign Affairs", September/October 2023

D. Charlotin (2023), *Large Language Models and the Future of Law*, August 2023

A. Engler (2023), *Early thoughts on regulating generative AI like chatgpt*, February 2023

L. Floridi, M. Chiriatti (2020), *GPT-3: Its nature, scope, limits and consequences*, in "Mind and Machine", vol. 30, 2020, n. 4

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

N. Helberger, N. Diakopoulos (2023), *ChatGPT and the AI Act*, in "Internet Policy Review", vol. 12, 2023, n. 1

M.E. Kaminski (2022), *Regulating the Risks of AI*, August 2022

G. Lo Sapio (2021), *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*", in "federalismi.it", 2021, n. 16

J. Mokander, J. Schuett, H.R. Kirk, L. Floridi (2023), *Auditing large language models: a three-layered approach*, in "AI & Ethics", 2023

24. È consentito, infatti, che detta sperimentazione sia avviata anche prima dell'entrata in vigore del regolamento AI Act, art. 53.1: «Gli Stati membri istituiscono almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in applicazione del presente regolamento».

M.M. Mollicone (2023), *Il rischio dell'intelligenza artificiale applicata. Modelli di allocazione a confronto*, in "Actualidad Jurídica Iberoamericana", 2023, n. 18

S. Pesucci (2022), *Diritto e intelligenza artificiale: opportunità e dilemmi nell'era della automazione*, in "Ristrutturazioni Aziendali", marzo 2022

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

G. Taddei Elmi (2021), *Il Quid, il Quomodo e il Quid iuris dell'IA. Una riflessione a partire dal volume "Diritto e tecnologie informatiche"*, in "Rivista italiana di informatica e diritto", 2021, n. 2

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0120 • articolo sottoposto a peer review • pubblicato in anteprima il 27 dic. 2023

Edoardo Colzani

Voto elettronico, problemi di sicurezza e rituali della democrazia

Nel presente contributo viene difesa la piena percorribilità del voto elettronico nel sistema costituzionale italiano, confutando la tesi sostenuta dai detrattori del voto elettronico per cui lo stesso sarebbe meno sicuro del voto analogico. L'Autore, anche attraverso il richiamo a casi concreti, mostra come il rischio di brogli elettorali sia insito in qualsivoglia procedura elettorale, a prescindere dalla natura dello strumento utilizzato per votare: ogni nuova tecnologia è stata sempre accompagnata da critiche e perplessità al riguardo. La sicurezza delle procedure di voto è condizionata secondo l'Autore dal grado di fiducia che i cittadini ripongono nel sistema. Si tratta di un obiettivo a cui la democrazia deve tendere ma rispetto al quale in molte occasioni essa si è rilevata debole e fallibile. La forza di una democrazia sta in tale consapevolezza e nella conseguente predisposizione di strumenti e procedure che tendano sempre più a garantire la sicurezza delle operazioni di voto e di scrutinio non solo in fase di espressione del voto ma anche nella successiva eventuale fase di controllo sugli esiti elettorali. Partendo da questa consapevolezza, secondo l'Autore, ci si renderà conto che non vi sono più motivi per ostacolare la sperimentazione del voto elettronico, pur a fronte di un continuo aggiornamento e di una implementazione della tecnologia e delle misure di sicurezza.

Democrazia – Voto elettronico – Sistemi di voto – Cittadinanza digitale

Electronic Voting, security problems and the rituals of democracy

The paper defends the full feasibility of electronic voting in the Italian constitutional system. Electronic voting can actually be considered as a secure voting tool as paper ballot voting. The author, through the reference to concrete cases, shows how the risk of electoral fraud is inherent in any electoral procedure, regardless of the nature of the instrument used to vote: every new technology has always been accompanied by criticisms and skepticism. According to the author, the security of voting procedures is conditioned by the trust citizens place in the normative system.The strength of a democracy lies in this awareness and in the consequent generation of tools and procedures which increasingly tend to guarantee the security of electoral operations not only during the casting of the vote but also in the subsequent possible phase of control over election results. Starting from this awareness, according to the author, we will realize that there are no more reasons to hinder the experimentation of electronic voting, even in the face of continuous updating and implementation of technology and security measures.

Democracy – Electronic voting – Voting system – Digital citizenship

L'Autore è avvocato, dottore di ricerca in Filosofia del diritto, assegnista di ricerca presso il Dipartimento di giurisprudenza dell'Università di Milano Bicocca

Tecnica e diritto sono i due fuochi attorno a cui si ridefinisce oggi, in forme nuove, il senso della democrazia e della libertà
(A. Soro, "Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale", Baldini e Castoldi, 2019)

1. Introduzione

Nel presente contributo intendo sostenere la percorribilità del voto elettronico in Italia attraverso la confutazione del principale argomento utilizzato dagli scettici, in particolare nel dibattito pubblico, per ostacolare l'utilizzo di tale sistema di votazione: la sicurezza del voto. Il dibattito sul voto elettronico in Italia riaffiora periodicamente in occasione delle principali competizioni elettorali[1], ma sino ad oggi la discussione non ha portato ad alcun risultato concreto, persistendo diffidenze e ritrosie. Ci sono state sperimentazioni, confinate nell'ambito locale[2], ma non s'è ancora visto un serio tentativo del legislatore nazionale di regolamentare la materia.

1. Da ultimo, con le medesime dinamiche e argomentazioni, il dibattito è stato sollevato da Elly Schlein anche con riguardo alla votazione per le primarie del Partito Democratico, dunque nell'ambito di votazioni interne ad un partito.
2. Il voto elettronico è stato adottato per numerose elezioni locali, sia con valore sperimentale che con pieno valore legale. La prima votazione elettronica si tenne nel 1997 in alcune frazioni del comune umbro di Amelia, in occasione dell'elezione di un comitato per la gestione di beni separati, e coinvolse circa un migliaio di cittadini. Il sistema di voto, sviluppato localmente per iniziativa del servizio elettorale, era già basato su tecnologia touch screen e, in anticipo rispetto al recente dibattito sull'importanza della traccia cartacea, era già dotato di una stampante ad aghi che produceva una busta sigillata per ciascun votante, contenente il voto espresso. I dati elettronici, invece, furono salvati su un floppy disk che, sigillato e timbrato, era destinato alla Prefettura, come abitualmente avviene per la trasmissione dei verbali cartacei. Come promesso ai cittadini e alla stampa i risultati delle elezioni vennero resi disponibili appena pochi secondi dopo la chiusura dei seggi; secondo il responsabile di questa iniziativa, inoltre, l'adozione su larga scala di questo sistema avrebbe permesso di risparmiare il 65% dei costi delle elezioni, soprattutto nelle spese per gli straordinari del personale di seggio e delle forze dell'ordine. Nello stesso anno anche il Ministero dell'Interno promosse, durante le consultazioni amministrative nei comuni valdostani di Arnad, Courmayeur, Issime, La Salle e Valsavaranche, l'utilizzo di dispositivi informatici (Carta del Cittadino, postazioni elettroniche per l'espressione del voto, urne elettroniche) in sostituzione a strumenti definiti "tradizionali" quali schede e certificati elettorali cartacei. A partire da queste esperienze pilota, nel giro di pochi anni il voto e lo scrutinio elettronico sono entrati nell'agenda del Ministero dell'Interno, degli enti locali e del mercato. Nelle elezioni regionali del 2000 gli elettori di una sezione di San Benedetto del Tronto hanno potuto provare un sistema touchscreen dopo aver votato con scheda di carta e matita copiativa; l'anno successivo, in occasione delle elezioni politiche, nei comuni sardi di Guamaggiore, Ortaceus, Serri ed Escolca,

Nella storia politica italiana il tema è riemerso in diverse occasioni, con una qualche risonanza mediatica, e per la precisione:

1) il referendum lombardo per l'autonomia svoltosi il 22 ottobre 2017 durante il quale per la prima volta è stato sperimentato un sistema di i-voting mediante tablet posizionati all'interno della tradizionale cabina elettorale;
2) il dibattito sul voto degli italiani all'estero e degli studenti fuori sede, ancora oggi di attualità grazie alle più recenti iniziative parlamentari dell'on. Riccardo Magi[3];
3) il referendum per l'eutanasia promosso mediante sottoscrizioni digitali[4];
4) le recenti elezioni politiche del 25 settembre 2022 durante le quali la lista Democrazia e Referendum di Marco Cappato ha promosso iniziative giudiziarie per il riconoscimento della sottoscrizione digitale delle liste elettorali[5].

Ho già avuto modo di individuare in un mio recente contributo[6] quelli che a mio avviso sono i principali ostacoli allo sviluppo del voto elettronico e le contraddizioni del sistema di voto in Italia.

In questa sede intendo interrogarmi sul tema della sicurezza del voto e delle procedure elettorali, chiedendomi che cosa significhi parlare di sicurezza del voto, da un lato, e se il voto analogico sia più sicuro del voto digitale.

Il tema della sicurezza del voto elettronico è del resto il principale argomento utilizzato per contrastare le proposte di rinnovamento delle procedure di voto: gran parte della classe politica e dell'opinione pubblica ancora non si sente sicura che un sistema elettronico sia altrettanto anonimo e affidabile quanto quello tradizionale[7]. Nell'affrontare il tema voglio in particolare soffermarmi in maniera più ampia sull'aspetto della trasparenza delle

---

i votanti sono stati invitati a ripetere la loro scelta su schede cartacee che accanto ai simboli dei partiti riportavano dei codici a barre leggibili con apposite penne ottiche, mentre a Novate Mezzola, in provincia di Sondrio, è stata proposta una macchina per il voto elettronico.

3. Proposta di legge Magi e Della Vedova: "Disposizioni concernenti l'esercizio del diritto di voto per le elezioni della Camera dei deputati, del Senato della Repubblica e dei membri del Parlamento europeo spettanti all'Italia nonché per i referendum da parte degli elettori che, per motivi di studio o di lavoro, hanno temporaneamente domicilio in una regione diversa da quella di residenza". La proposta, presentata il 13 ottobre 2022, è allo stato all'esame della Commissione Affari Costituzionali della Camera.
4. «Il Presidente Maroni ha ricordato in proposito che si è svolta una regolare gara, sulla base quale sono state acquistate 24.000 voting machine, una sorta di tablet, che hanno consentito di effettuare il voto elettronico in tutti i seggi, attraverso una procedura molto semplice, con l'utilizzo del touch screen. La votazione si è svolta in maniera assolutamente regolare durante tutto l'arco della giornata. Alcuni problemi si sono verificati al momento della chiusura dei seggi, non per un malfunzionamento del sistema, ma a causa del fattore umano. Alcuni presidenti di seggio non hanno rispettato la procedura e hanno inizializzato le tre voting machine di ciascun seggio con lo stesso codice; conseguentemente il computer non ha letto i codici, scartando i risultati delle voting machine successive alla prima. In secondo luogo, alcuni Comuni hanno allestito una sala insufficiente per la ricezione dei verbali e delle chiavette elettroniche, per trasmettere i risultati immediatamente al livello centrale della Regione, per cui si sono formate lunghe code di coloro che portavano le chiavette dai seggi. Il Presidente ha inoltre fatto presente che la sperimentazione ha avuto nel complesso un esito soddisfacente e che il know how acquisito è a disposizione del Ministro dell'interno per un eventuale utilizzo in altre elezioni. Il Ministero dell'interno è stato infatti coinvolto, per il contemporaneo svolgimento in 17 Comuni del referendum per le fusioni ed ha quindi verificato le procedure ed il sistema di voto. Successivamente le voting machine sono state ricondizionate e messe a disposizione gratuitamente del sistema scolastico regionale, anche ai fini del collegamento con le LIM (lavagne interattive multimediali)». Cfr. *XVII legislatura. Bollettino delle giunte e delle commissioni parlamentari. Commissione parlamentare per le questioni regionali. Indagine conoscitiva sull'attuazione dell'articolo 116, terzo comma, della Costituzione, con particolare riferimento alle recenti iniziative delle regioni Lombardia, Veneto ed Emilia-Romagna*.
5. Colzani 2023.
6. Colzani 2022.
7. Cfr. Sarais 2008.

procedure elettorali e sulla fiducia che i cittadini ripongono in tali procedure e più complessivamente nel sistema[8].

La tesi che intendo sostenere è che la sicurezza del voto, sia esso analogico o digitale, è un obiettivo a cui la democrazia deve tendere ma rispetto al quale in molte occasioni essa si è rivelata debole e fallibile. Un voto "sicuro al 100%" è un obiettivo irrealizzabile, sia che si voti con la classica scheda elettorale e matita copiativa sia che si ricorra a strumenti di i-voting o e-voting[9].

In buona sostanza, ove il legislatore italiano voglia dare spazio al voto elettronico deve necessariamente accettare un compromesso che passa per un alleggerimento dei vincoli che una rigida interpretazione dell'art. 48 della Costituzione comporta e che allo stato costituiscono una insormontabile barriera per il cambiamento delle procedure di espressione del voto[10]. Come si dimostrerà peraltro – e in ciò viene in soccorso il modello americano – ad una attenuazione dei vincoli costituzionali che dovranno essere reinterpretati alla luce anche del cambiamento tecnologico dovrà necessariamente seguire un rinforzato sistema di controlli (in questo senso è illuminante la sentenza del Tribunale Costituzionale Tedesco del 3 marzo 2009). Si consideri, peraltro, come in molti Paesi europei, i concetti di segretezza e personalità del voto sono interpretati con maggior disinvoltura e la diffusione del voto per corrispondenza e per procura lo dimostra.

La forza di una democrazia sta in tale consapevolezza e nella conseguente predisposizione di strumenti e procedure che tendano sempre più a garantire la sicurezza delle operazioni di voto e di scrutinio non solo in fase di espressione del voto ma anche nella successiva eventuale fase di controllo sugli esiti elettorali. Partendo da questa consapevolezza, ci si renderà conto che non vi sono più motivi per ostacolare la sperimentazione del voto elettronico, pur a fronte di un continuo aggiornamento e di una implementazione della tecnologia e delle misure di sicurezza[11].

Affronterò di seguito il tema della sicurezza del voto, dimostrando come storicamente non esista una procedura di voto che non sia vulnerabile: sarà affrontato il tema della sicurezza del voto a partire dall'analisi dei cosiddetti brogli elettorali.

Quale che sia il mezzo attraverso cui il voto viene espresso, la storia e la comparazione con esperienze diverse da quella italiana, ci ha offerto numerosi casi di contestazioni sul voto. In taluni casi, la responsabilità è da additare a un fattore umano, errori nella filiera di controlli da parte del personale addetto ai

8. Si segnalano, per una migliore contestualizzazione del tema, i seguenti contributi: Zurita Aldeguer 2001, Nevola 2007.
9. Il primo rappresenta il voto in Internet, espresso da remoto dinanzi al proprio computer (generalmente indicato con i-voting), il secondo rappresenta il voto effettuato in cabina, nel seggio, utilizzando un videoterminale in luogo della scheda cartacea (il c.d. e-voting).
10. La sensibilità costituzionale italiana per il voto segreto ha portato per due volte la disciplina del voto degli italiani all'estero davanti alla Consulta, con un conflitto di attribuzione poco dopo l'entrata in vigore delle norme e una questione di legittimità ben più recente. Entrambi i casi hanno dato luogo a ordinanze di inammissibilità, ma nella prima la Corte ha rilevato che, se si fossero ritenute illegittime le norme sul voto per corrispondenza per violazione dell'art. 48 Cost. (ipotesi non esclusa), si sarebbe reso «assai più difficile l'espressione del voto degli italiani residenti stabilmente all'estero, pur titolari del diritto di voto e quindi componenti del corpo elettorale su cui calcolare il quorum» del referendum; nell'altra, il giudice delle leggi ha ammesso che le censure si riferivano a «oggettive criticità della normativa denunciata quanto al bilanciamento della "effettività" del diritto di voto dei cittadini residenti all'estero con gli imprescindibili requisiti di personalità, libertà e segretezza del voto stesso». Così si è di fatto riconosciuto che il voto per corrispondenza presenta profili critici in materia di garanzia di segretezza: si possono considerare recessivi rispetto ai vantaggi del rendere accessibile il diritto di voto a chi diversamente non riuscirebbe a esercitarlo, ma non per questo spariscono o sono facilmente risolvibili. Cfr. Maestri 2020.
11. Come noto, l'Estonia è sotto questo punto di vista uno dei paesi più all'avanguardia. La costante implementazione delle misure di sicurezza. Durante il convegno "*E-vota – Verso il voto elettronico per l'innovazione democratica*", tenutosi alla Camera dei Deputati il 12 marzo 2019, il rappresentante dell'Estonia Tarvi Martens ha effettivamente esplicitato che la sicurezza è sempre in fase di implementazione.

seggi, in altri casi l'errore è da addebitarsi a un mal funzionamento delle macchine.

Sosterrò altresì che il grado di maturità di una democrazia sia correlato alla capacità di prevenire, da un lato, accertare e sanzionare, dall'altro, eventuali brogli elettorali che sono rischi connaturati alla democrazia stessa.

Anzi, una democrazia è matura laddove vi è presa di coscienza dei margini di errore, sia esso umano che connesso a una macchina, ed elaborazioni di strumenti di prevenzione e contrasto di tali margini di errori. Laddove non sia possibile ridurre il rischio brogli, ciò che ci si aspetta è quantomeno – ed ecco che si ritorna alla già richiamata sentenza della corte costituzionale tedesca – un sistema di procedure trasparenti e soggetto a controllo, che consentano quantomeno ex post di denunciare le anomalie e pretendere un riconteggio dei voti.

Se da un lato dunque i brogli elettorali possono compromettere la fiducia degli elettori nei processi elettorali, dall'altro, si può affermare che un articolato sistema di controlli e garanzie consente il ripristino della dignità della macchina democratica e consolida la fiducia del cittadino nelle istituzioni.

2. Pro e contro del voto elettronico

Discutere di voto elettronico e valutare l'opportunità della sua legittimazione nel sistema elettorale italiano implica una valutazione a monte di vantaggi e svantaggi connessi allo strumento e una attività preliminare di valutazione dei rischi connessi allo strumento nell'ottica della loro prevenzione e gestione secondo modalità trasparenti e verificabili (sul punto si ritornerà più ampiamente).

I vantaggi del voto elettronico rispetto al tradizionale voto su scheda elettorale cartacea possono essere sintetizzati come segue:

1) semplificazione delle procedure di voto;
2) abbattimento dei costi connessi alle procedure elettorali;
3) maggiore accessibilità da parte degli elettori;
4) garanzia di un più preciso conteggio dei voti;
5) tempestività dei risultati;
6) riduzione dei casi controversi (voti nulli o dubbi – sopravvive invece la c.d. scheda bianca).

Altrettanto noti, tuttavia, sono i principali difetti dei sistemi di voto elettronico finora sperimentati: si tratta essenzialmente di potenziali rischi per la segretezza, di possibili frodi provenienti dall'interno o dall'esterno, perdita/aggiunta di voti espressi, problemi di trasparenza e di fiducia nel sistema legati alla proprietà dei software e dell'hardware. L'esperienza americana ci insegna che le principali problematiche con cui distretti, contee, Stati e, in misura minore, il governo federale devono fare i conti sono essenzialmente riconducibili a tre fenomeni. In primo luogo, si segnala il "naturale" invecchiamento delle macchine, che non solo riduce la precisione e l'affidabilità del conteggio dei voti, ma rende anche gli impianti astrattamente più vulnerabili a manomissioni; in secondo luogo, quale conseguenza della vulnerabilità legata all'obsolescenza delle macchine, i tentativi di modificare il risultato delle elezioni tramite interventi maligni sull'equipaggiamento elettorale operati a distanza; ed infine un più generale sentimento diffuso di sfiducia verso l'amministrazione pubblica[12].

Preso atto dunque dei pregi e dei difetti del voto elettronico, l'opzione per quest'ultimo è, a mio avviso, dettata anzitutto da principi di efficienza e rapidità di gestione del processo elettorale.

Ove si voglia esercitare detta opzione, occorrerà poi procedere a un bilanciamento dell'efficienza con i principi costituzionalmente tutelati in materia di diritto di voto.

Nel far ciò al legislatore è richiesto un approccio pragmatico: così come accade per il voto cartaceo, ugualmente per il voto elettronico l'elettore non può qui avere alcuna certezza assoluta sulla regolarità dello spoglio delle schede, ma ragionevolmente può solo confidare nell'osservanza delle procedure affinché i sigilli non siano manomessi[13].

3. Sicurezza del voto

Al fine di comprendere che cosa si intenda per voto sicuro e come il concetto di sicurezza si declini con riguardo alle procedure elettorali, appare opportuno muovere da una succinta disamina dei principali documenti internazionali che si occupano del diritto di voto. Uscendo dunque dalla dimensione nazionale, il tema va approcciato da una

12. Cfr. Trancossi 2020.
13. Sul punto si segnala un interessante tentativo di pensare un sistema di votazione elettronica basato su blockchain in Ladu 2023.

prospettiva di più ampio respiro, evidenziando come la tensione verso la sicurezza delle procedure di voto è una caratteristica che accomuna tutti gli Stati democratici.

Qui di seguito una elencazione dei principali documenti internazionali e degli articoli appositamente dedicati al tema.

L'art. 21 della Dichiarazione Universale dei diritti dell'uomo al comma 3 afferma che «La volontà popolare è il fondamento dell'autorità del governo: tale volontà deve essere espressa attraverso periodiche e veritiere elezioni, effettuate a suffragio universale ed eguale, ed a voto segreto, o secondo una procedura equivalente di libera votazione». L'art. 25 del Patto internazionale relativo ai diritti civili e politici parla di elezioni periodiche, veritiere, effettuate a suffragio universale ed eguale, ed a voto segreto, che garantiscano la libera espressione della volontà degli elettori. L'art. 3 del Protocollo 1 CEDU recita: «Le alte parti contraenti si impegnano a organizzare, a intervalli ragionevoli, libere elezioni a scrutinio segreto, in condizioni tali da assicurare la libera espressione dell'opinione del popolo sulla scelta del corpo legislativo». Infine, l'art. 39 della Carta dei diritti fondamentali dell'Unione europea afferma che «Ogni cittadini dell'Unione ha il diritto di voto e di eleggibilità alle elezioni del Parlamento europeo nello Stato membro in cui risiede, alle stesse condizioni dei cittadini di detto Stato. I membri del Parlamento europeo sono eletti a suffragio universale diretto, libero e segreto».

Dalla lettura di quanto sopra emerge che il voto sicuro si caratterizza come quel voto che scaturisce da elezioni periodiche, veritiere, a voto segreto, che garantiscano una libera espressione della volontà dell'elettore. Tali principi, in ambito italiano trovano conferma nell'art. 48 della Costituzione il cui primo comma chiaramente afferma che «Il voto è personale ed eguale, libero e segreto».

La sicurezza del voto si declina dunque, da un lato, come sicurezza delle procedure elettorali, dall'altro, come libera espressione del voto da parte dell'elettore all'interno della cabina elettorale. In tale duplice aspetto, formale (la correttezza delle procedure e il regolare svolgimento delle elezioni) e sostanziale (la possibilità per l'elettore di esprimere un voto consapevole e libero da condizionamenti) si concretizza il rito della democrazia.

Dal punto di vista delle forme della democrazia, l'esercizio del diritto di voto si presenta come un rito ammantato dal carattere della solennità[14]. Il voto è una sorta di rito collettivo in cui ogni cittadino è chiamato a esprimersi nella consapevolezza di stare adempiendo un dovere giuridico connesso alla funzione pubblica che è chiamato a svolgere, perché e in quanto membro del popolo: la funzione pubblica dell'espressione del voto deve avvenire anch'essa pubblicamente, perché solo così ogni elettore sentirà di adempiere un obbligo morale inderogabile, di anteporre l'interesse pubblico ai propri interessi privati. Ci si aspetta in sostanza che l'elettore esprima il proprio voto secondo criteri razionali, come se a votare fosse solo lui e dalla sua scelta dipendesse l'esito della consultazione: ammettendo ciò, ne consegue che il dovere di votare in quanto dovere pubblico va adempiuto in pubblico, sotto la sorveglianza del pubblico.

Dal punto di vista sostanziale, la sicurezza del voto, implica invece che il voto sia espresso dall'elettore in maniera libera da condizionamenti di alcun tipo.

Ricapitolando, dunque, voto sicuro è, in primo luogo, il voto che viene espresso nell'ambito di procedure pubbliche e trasparenti, idonee a garantire la massima regolarità dal punto di vista formale. In secondo luogo, voto sicuro è quello che viene espresso dall'elettore nel segreto dell'urna, in maniera consapevole e libera da condizionamenti.

Una siffatta ricostruzione del concetto di "voto sicuro", che tenga ben distinta la fase preliminare all'espressione del voto e la fase vera e propria di espressione del voto, fa emergere una contraddizione: il principio della segretezza del voto infatti contrasta col principio di pubblicità della procedura. A tal proposito, va rilevato come prima dell'avvento della scheda cartacea il sistema elettorale prevedesse l'espressione del voto in forma orale, nell'ottica di un rafforzamento dell'elezione come un rito collettivo in cui il voto era pubblico e verificabile.

Eppure, in particolar modo con l'ampliamento della base dei votanti e dunque con l'introduzione del suffragio universale, s'è avvertita la necessità di una maggiore garanzia del singolo cittadino

14. Frosini 2021, pp. 2-3.

nell'espressione della propria volontà[15]: la necessità che il voto di ciascun elettore non fosse l'esito di un comportamento cedevole, e accondiscendente di braccianti e operai nei confronti delle richieste elettorali dei propri padroni e datori di lavoro, storicamente condusse all'introduzione di legislazioni elettorali che assicuravano l'anonimato degli elettori. Il voto segreto veniva dunque a configurarsi quale strumento di difesa dalle pressioni nei confronti dei cittadini più deboli, si afferma per tutelare gli elettori da influenze esterne, combattere la corruzione elettorale, che si estendeva man mano che si allargava l'elettorato attivo e garantire, infine, la libera espressione della libertà del votante[16].

4. I brogli elettorali

Il tema della sicurezza del voto implica dunque la prevenzione di manipolazioni/alterazioni con riguardo alla procedura elettorale, da un lato, all'espressione del voto, dall'altro. Esistse, poi, un terzo aspetto legato al tema della sicurezza, ossia il controllo dei risultati.

Ricapitolando, dunque, quando parliamo di sicurezza del voto dobbiamo fare riferimento a tre aspetti:

1) sicurezza delle operazioni elettorali;
2) sicurezza della fase di espressione del voto;
3) sicurezza della fase successiva di conteggio dei voti.

Attraverso questo terzo aspetto della sicurezza, intendo fare un cenno al tema dei brogli elettorali per dimostrare come l'esistenza dei brogli elettorali, da un punto di vista storico presenti (anche solo come minaccia) in qualsivoglia competizione elettorale, sia argomento valido a confutare le preoccupazioni sul voto elettronico.

In qualsiasi contesto istituzionale e in qualsiasi periodo storico il tema dei brogli ha trovato spazio. Il tema dei brogli nelle elezioni affonda le radici nell'antichità tanto che già nella Grecia del V secolo a.C. si registrarono primi casi: i frammenti di terracotta su cui veniva inciso il nome dell'ostracizzato recavano spesso incisioni a cura della medesima mano. Il broglio è il principale argomento utilizzato dalle forze politiche sconfitte per cercare di delegittimare l'avversario politico. Come ha evidenziato la sociologa Letizia Caporusso[17], far leva sullo strumento retorico del broglio serve a mobilitare il proprio elettorato, coagulandolo entro una prospettiva di vittimismo, nonché a gettare discredito e seminare sospetti, non tanto sugli avversari politici quanto sul sistema *tout court*, sistema che, peraltro, entrambi gli schieramenti hanno contribuito a delineare: la legittimazione di una procedura, al pari della legittimazione del potere, riposa su una base morale condivisa che trascende ed è successiva alla sua istituzionalizzazione: quando questa condivisione dei valori ultimi viene meno, il dialogo fra le forze politiche rischia in prima istanza la paralisi, ma in seconda battuta deve – presto o tardi – accettare la rinegoziazione delle regole del gioco democratico, ivi comprese quelle meramente procedurali.

I brogli elettorali, dunque, prescindono dalla modalità, analogica o digitale, con cui il voto può venire espresso. Si tratta di un tema che non solo viene utilizzato per delegittimare l'avversario politico ma che storicamente è stato utilizzato per avversare ogni cambiamento in materia elettorale e che dunque non deve stupire se oggi viene utilizzato per demonizzare il voto elettronico. Ancora una volta richiamando le considerazioni di Marco Schirippa è di estrema utilità fare un cenno all'avvento del voto cartaceo, in sostituzione del voto espresso in forma pubblica e orale, e alle diffidenze che hanno accompagnato questa «prima forma di tecnologia applicata al processo elettorale»: tale sistema non garantiva pienamente né la segretezza del voto né la sua autenticità, poiché vi si poteva riconoscere la scrittura dell'elettore, votare, in sua vece o, peggio ancora, alterare o sostituire la scheda senza lasciare traccia del misfatto[18].

È interessante notare come la storia delle macchine da voto e dei sistemi di voto sia caratterizzata da un costante alzarsi di critiche sull'idoneità dello strumento a garantire la regolarità delle procedure di voto.

Le prime "macchine di voto" risalgono alla fine del XIX secolo e funzionavano attraverso un sistema di leve: sebbene non siano più in

15. Per un approfondimento si rimanda a Pinelli 1996.
16. Schirripa 2021, p. 25.
17. Caporusso 2008.
18 Schirripa 2021, p. 25.

produzione, alcuni dispositivi di questo tipo sono tutt'oggi in uso negli Stati Uniti. L'interfaccia delle *lever machine* mostra simultaneamente tutti i quesiti elettorali e tutti i nomi dei candidati: l'elettore posiziona la leva in corrispondenza della scelta desiderata e all'uscita dalla cabina il meccanismo di spoglio incrementa di una unità il conteggio per quella determinata opzione. Orbene, la critica ricorrente nei confronti di questo tipo di macchina è che questo modo di procedere non consente il riconteggio dei voti, posto che questi vengano registrati esclusivamente in modo aggregato.

Un'altra modalità di conteggio meccanico dei voti è rappresentata dalle punzonatrici: in questo caso ogni cabina elettorale è dotata di un libretto che viene posto sopra una scheda perforabile (*votomatic*) o di schede con nomi prestampati (*datavote*), l'elettore utilizza uno stilo per bucare la scheda in corrispondenza dei nomi dei candidati prescelti e le singole schede, che in questo caso rimangono a disposizione per eventuali controlli e riconteggi, vengono poi scrutinate da un apposito dispositivo meccanico. I limiti di questa procedura sono essenzialmente riconducibili all'errato posizionamento del libretto sopra la scheda, alla punzonatura incompleta e ai cosiddetti "coriandoli" vaganti: le presidenziali americane del 2000 hanno evidenziato tutte queste problematiche tanto che molte contee hanno deciso – a quarant'anni dalla loro introduzione – di rottamare le *punch-card*.

Al di qua dell'oceano, invece, paesi come il Belgio e l'Olanda hanno utilizzato fin dagli anni Ottanta sistemi elettronici per lo spoglio dei voti: non dissimili dall'idea sottostante le macchine a leve, i dispositivi elettronici a registrazione diretta (*direct recording electronic*, o *DRE*) conteggiano in modo aggregato i voti attribuiti a ciascun partito o candidato, con l'unica differenza che l'elettore, anziché azionare una leva meccanica, preme il pulsante corrispondente alla propria scelta.

Recentemente anche questa procedura è stata messa in discussione da piccoli ma determinati gruppi di attivisti: nel 2004 il governo irlandese è stato costretto a posticipare a data da definirsi l'utilizzo di macchine DRE, per il cui acquisto erano stati investiti oltre cinquanta milioni di euro; nel 2007 il Ministero degli Interni olandese ha deciso di ritirare le licenze e le macchine di entrambi i fornitori nazionali, in uso da circa vent'anni, prefigurando il ritorno a carta e matita rossa fino alla stesura di nuove linee guida che definiscano puntualmente gli standard di sicurezza e trasparenza.

Le critiche mosse nei confronti dei dispositivi a registrazione diretta del voto si collocano sostanzialmente in due ordini di problemi: da una parte viene avvertita la necessità di poter operare, come prassi e non solo come eccezione, un riconteggio parziale o totale dei voti[19]; dall'altra gli attivisti si schierano contro l'utilizzo di software proprietario le cui modalità operative sono sconosciute non solo al pubblico, ma anche all'istituzione che lo utilizza[20]. Entrambe le osservazioni riposano sulla necessità di una gestione non esclusiva dell'evento elettorale: ciascun singolo cittadino (o per lo meno

19. La prima questione viene affrontata dai tecnici evocando l'introduzione di stampanti che consentano all'elettore di verificare la propria scelta prima che questa venga registrata dal sistema elettronico: tali prove fisiche andrebbero poi utilizzate per verificare, anche a campione, che i dati registrati dalle macchine siano conformi alle schede cartacee approvate dai votanti, unico supporto che dovrebbe avere valore legale in caso di difformità o contestazioni. Anche questa soluzione viene messa in discussione, posto che numerose ricerche empiriche dimostrano la tendenza dei votanti a non effettuare il controllo sulle stampate; tuttavia, la responsabilità di non riconoscere eventuali malfunzionamenti ricadrebbe, in questi casi, non più sui programmatori e sui produttori di dispositivi di voto, ma sugli elettori stessi.

20. Il secondo argomento evoca una serie di cambiamenti paradigmatici nella disciplina della sicurezza, informatica e non. Storicamente l'inaccessibilità di un sistema viene garantita dall'ignoranza rispetto al suo funzionamento, secondo il modello conosciuto come *security by obscurity* (sicurezza attraverso l'oscurità), spinto fino agli eccessi ironicamente descritti da Jeff Raskin, che coniò l'acronimo TIC (*Total Internal Confusion*) per descrivere la situazione in cui neanche chi lavora sul sistema conosce esattamente i suoi algoritmi. Il modello della sicurezza attraverso l'oscurità venne messo in discussione già alla fine del XIX secolo con la nascita della crittografia, approccio secondo il quale il "nemico" può conoscere tutto di un piano, tranne la chiave necessaria a decifrarne il codice. Anche questo modello è stato recentemente criticato, in nome di una maggiore trasparenza nelle procedure: se dunque da una parte non appare auspicabile uno scenario nel quale le operazioni elettorali

i suoi rappresentanti, nella forma di un'autorità di certificazione indipendente) deve essere in grado di conoscere cosa avviene del suo voto dal momento in cui questo viene espresso al momento in cui si procede allo scrutinio. Anche in questo caso risulta dunque cruciale il ruolo delle commissioni elettorali (che in molti paesi, a differenza dell'Italia, sono svincolate dagli organi di governo) e degli osservatori, indipendenti e specificamente formati.

Nel sistema italiano, principale oggetto della presente analisi, peraltro, la preoccupazione è accentuata dalle peculiarità del contesto sociale come viene esplicitamente chiarito nella relazione illustrativa di una proposta di legge datata 2015 espressamente volta a introdurre una serie di interventi normativi atti a rendere il processo elettorale più trasparente e meno soggetto a distorsioni e inquinamenti del voto[21]: «Nel nostro Paese il voto di scambio politico-mafioso, l'annullamento seriale di schede, schede già votate nell'urna prima dell'apertura dei seggi e persone decedute che votano sono solo alcuni dei fenomeni che puntualmente inquinano il risultato delle elezioni, mettendo a rischio la stessa funzionalità della democrazia. La tutela del processo elettorale sta alla base di qualsiasi rivoluzione democratica, in assenza della quale ogni sforzo di cambiamento sarà vanificato dall'azione di gruppi criminali e dalla connivenza di esponenti politici. Quasi a ogni tornata elettorale, sia essa a valenza locale che nazionale, puntualmente vengono denunciati da più parti brogli elettorali che, vista l'esiguità con la quale alcune elezioni sono state vinte, potrebbero modificare l'intero esito elettorale». La fondamentale rilevanza di questo aspetto risulta ancora più grave in un sistema elettorale con pesanti correttivi maggioritari, qual è il premio di maggioranza, nel quale, anche pochi voti in più potrebbero garantire la maggioranza dei seggi parlamentari e con essa la possibilità di formare il Governo.

Al di là della contingenza in cui fu elaborata la proposta di legge e dunque degli specifici episodi di cronaca che hanno in qualche modo sollecitato l'intervento, è interessante evidenziare gli sforzi per rafforzare il sistema di tutela del processo elettorale e le preoccupazioni che ancora accompagnano il tradizionale sistema di voto, tanto da portare a ripensare addirittura la conformazione stessa della tradizionale cabina elettorale e dell'urna elettorale.

Si legge sul punto sempre nella relazione: «Le tendine preposte a coprire le cabine elettorali e la conformazione stessa delle cabine elettorali sono un altro tema molto dibattuto da anni nel nostro Paese. In Italia, infatti, a differenza di numerosi altri Paesi, le cabine elettorali sono chiuse da tutti e quattro i lati, grazie all'uso della tendina posteriore che copre le spalle dell'elettore. Questo sistema, se da un lato può assicurare la segretezza del voto, al medesimo tempo garantisce fin troppe possibilità di manipolare la scheda elettorale, rendendo riconoscibile il voto stesso. In molti Paesi occidentali, e non solo, questo sistema è stato ampiamente superato prevedendo cabine elettorali sprovviste di tendine e coperte solo lateralmente e frontalmente. In questo modo è impossibile falsificare o rendere riconoscibile il proprio voto senza essere scoperti dai membri dell'ufficio elettorale di sezione. Per questo motivo è modificata la cabina elettorale, prescrivendo che essa sia rivolta verso l'esterno della sezione elettorale e riparata solo su tre lati, lasciando quindi visibile la parte posteriore. Rispetto alle pratiche vigenti è dunque escluso l'utilizzo di tendine che coprano la schiena dell'elettore al momento della votazione. L'urna elettorale stessa ha posto non pochi problemi. Essendo completamente di cartone bianco, essa impedisce di vedere se all'interno vi siano schede elettorali o no. Non sono infatti rari i casi in cui, negli istanti immediatamente prima l'inizio o dopo la fine delle votazioni, sono inserite molte schede elettorali

siano demandate a privati gelosi dei propri "segreti aziendali", anche l'utilizzo della crittografia entro un sistema perfettamente accessibile non convince gli scettici.

21. Proposta di legge d'iniziativa dei deputati Nesci, Nuti, Basilio, Bonafede, Cecconi, Chimienti, Colletti, Colonnese, Cominardi, Cozzolino, D'Ambrosio, De Lorenzis, Di Benedetto, Di Maio, Di Stefano, D'Uva, Ferraresi, Fico, Liuzzi, Lombardi, Lorefice, Micillo, Parentela, Scagliusi, Sibilia, Spadoni, Terzoni, Tofalo, Zolezzi "Modifiche al testo unico di cui al decreto del Presidente della Repubblica 30 marzo 1957, n. 361, concernente l'elezione della Camera dei deputati, e al testo unico di cui al decreto del Presidente della Repubblica 16 maggio 1960, n. 570, concernente l'elezione degli organi delle amministrazioni comunali, nonché altre norme in materia elettorale presentata l'11 maggio 2015".

già votate. A tale fine si prevedono urne elettorali costituite da materiale semitrasparente, in modo da non poter verificare i voti espressi ma al tempo stesso in grado di garantire la presenza di schede prima dell'inizio delle votazioni».

5. Meccanismi di difesa e controllo del voto

Il rischio di frodi e brogli elettorali è connaturato alla democrazia a prescindere dalla tecnologia utilizzata. Anzi, affermo la tesi per cui tanto più una democrazia è matura quanto più sia possibile per una qualsiasi forza politica sollevare una accusa di frode elettorale cui segua una procedura di verifica e controllo i cui esiti portano a un rafforzamento e consolidamento della democrazia stessa. Richiamo di seguito, condividendolo, un passo dell'analisi del professor André Ramos Tavares all'interno di uno studio sulla crisi della legittimazione elettorale[22]. Dopo aver passato in rassegna le esperienze di diversi Stati (tra cui anche Italia[23] e Stati Uniti[24]), lo studioso conclude che l'accusa di frode farebbe parte della retorica democratica come un nuovo e frequente armamentario di attacco all'avversario e al risultato non desiderato dall'accusatore; peraltro, il sospetto di brogli trova la sua ragione in una mutua diffidenza tra i concorrenti della competizione elettorale. Egli sostiene inoltre la tesi altrettanto condivisibile per cui «può essere impossibile e irrealistico un processo perfetto, ermeticamente sigillato e immune alle contestazioni»[25]. Come evidenziato da Lucio Pegoraro, sin dai loro primordi i Parlamenti hanno ricercato il modo di assicurare la correttezza del processo elettorale: dapprima, quando il governo era del re e non c'era rapporto fiduciario, avocando a sé il compito di controllare la loro stessa composizione poi dislocando il relativo potere fuori dal Parlamento a organi terzi quali la magistratura ordinaria, il Tribunale costituzionale o organi *ad hoc* – nei paesi dell'area asiatica e America latina la tendenza è quella di creare veri e propri tribunali/commissioni elettorali, il modello europeo è quello della attribuzione della vigilanza sulle operazioni elettorali e la decisione sui relativi ricorsi alle Corti costituzionali.

Oggi, peraltro, la problematica del controllo sulle elezioni va oltre la mera verifica dei risultati ed anzi attiene alla fase antecedente e per la precisione i controlli sulla correttezza della campagna elettorale, dell'uso della propaganda politica, lo svolgimento delle consultazioni. La nozione di "controllo" riferita al meccanismo elettorale è dunque ampia e attiene sia alla fase preparatoria delle elezioni, alla competizione elettorale, sia alle operazioni di voto, sia da ultimo alle operazioni di scrutinio. Si noti dunque come la problematica del controllo delle elezioni abbia oggi risvolti prima sconosciuti, andando ben oltre la mera verifica dei risultati per coprire anche la correttezza delle campagne elettorali e l'uso della propaganda politica. È interessante sul punto la riflessione di Pegoraro sulla nozione di controllo, esaminata a partire da una prospettiva di tipo comparatistico: « Se si dà alla parola controllo il senso tecnico di attività di riscontro corredata da potenziale sanzione favorevole o sfavorevole, certamente esso è riduttivo per l'analisi comparata in materia di elezioni. Se viceversa, sulla base della ricognizione dell'esistente, se ne allarga il significato alle varie attività svolte in molteplici paesi da organi specializzati – quale che sia il loro nomen e la loro natura funzionale – ecco che risulta più giustificato parlare di controllo delle elezioni ricomprendendo nella nozione anche attività amministrative/gestionali e giurisdizionali»[26].

Da ultimo occorre dare atto delle condivisibili osservazioni della corte tedesca nella già richiamata pronuncia del 3 marzo 2009 per cui in una

22. Ramos Tavares 2011.

23. Viene richiamato in particolare il caso delle elezioni 2006 nelle quali Silvio Berlusconi sollevò dubbi in ordine al risultato elettorale che assegnava la vittoria a Romano Prodi.

24. Viene richiamato in particolare il caso del 2000 delle elezioni che hanno visto contrapposti George W. Bush e Al Gore, decretando la vittoria del primo, cui andò la maggioranza dei seggi nonostante Gore avesse ottenuto il maggior numero di voti popolari. Più nello specifico, si evidenzia come la legittimità dell'elezione di Bush fu contestata da Gore per i dubbi sul conteggio dei voti in Florida, all'epoca governata da Jeb Bush, il fratello di George.

25. Ramos Tavares 2011, p. 28.

26. Pegoraro 2011, p. 352.

forma di governo parlamentare «la pubblicità del voto è la condizione essenziale per la formazione di una volontà politica democratica. Essa assicura la conformità all'ordinamento e il controllo delle procedure di voto e crea pertanto un presupposto basilare per la motivata fiducia dei cittadini nel corretto svolgimento delle votazioni; perciò tutti i passaggi essenziali di un'elezione devono essere soggetti a un possibile controllo pubblico. La presentazione dei candidati, lo scrutinio (in relazione all'espressione del voto e alla sua segretezza) e la determinazione del risultato devono, in quanto passaggi essenziali, poter essere verificati da tutti i cittadini in modo effettivo e senza che sia necessaria una specifica conoscenza tecnica.

6. L'ipocrisia del legislatore italiano

Quanto sopra premesso in tema di voto elettronico, appare da stigmatizzare l'atteggiamento ipocrita del legislatore italiano sotto tre punti di vista:

1) le modalità di voto all'interno del Parlamento;
2) le modalità di voto dei cittadini italiani all'estero;
3) le timide aperture solo verso i referendum.

In primo luogo, è da rilevare come già dal 1971 il Parlamento italiano ha introdotto per le proprie votazioni il voto elettronico[27]. Per quanto si tratti di una platea ristretta di aventi diritto al voto e per quanto eventuali problemi di sicurezza possano essere agevolmente superati semplicemente ripetendo la votazione, non può comunque negarsi che il voto elettronico di tipo deliberativo, rispetto a quello elettivo, ha una maggiore interazione, in concreto, con tutto l'assetto e il sistema politico-istituzionale in quanto consente alla sovranità popolare, nel *continuum* rappresentativo tra eletti ed elettori, di esprimersi[28]. Orbene, la votazione elettronica per il Parlamento rientra tra i sistemi di votazione palese previsti dai Regolamenti delle due Camere. Nello specifico la votazione con dispositivi elettronici (senza o con registrazione dei nomi) è spesso integrata ad altre modalità di voto palese come l'appello nominale e l'alzata di mano (artt. 53, 54 Reg. Cam. e 114, 115, 116 Reg. Sen.). Inoltre il voto elettronico può essere adottato anche in caso di votazione a scrutinio segreto. Il voto elettronico che i parlamentari esprimono presso le Camere è una forma di e-voting, una delle due facce del voto elettronico nel mondo. Il voto elettronico si presenta come un valido strumento perché consente il conteggio dei voti in modo più rapido rispetto alle altre modalità di votazione. La votazione elettronica avviene tramite apposite apparecchiature installate davanti al seggio di ogni parlamentare. Prima di procedere alla votazione, per la quale è previsto un periodo di preavviso per ragioni organizzative, ogni parlamentare dispone di una tessera di identificazione. Al momento della votazione il parlamentare deve inserire la tessera nell'apposita fessura del seggio e successivamente premere il pulsante corrispondente al voto che è intenzionato a esprimere («sì», «no», «astenuto»). Terminata la votazione, viene mostrato un elenco dei votanti con l'indicazione del voto espresso da ciascuno. Tale documento viene prima consegnato al Presidente (della Camera o del Senato), il quale ufficializza l'esito della votazione, infine pubblicato nei resoconti della seduta.

Si segnala che, durante il periodo pandemico, per agevolare l'attività parlamentare s'è addirittura dibattuto circa la possibilità di un voto da remoto per i parlamentari. Anche in questo caso, tuttavia, la questione non è stata di pronta definizione: da un lato si trattava infatti di dare la garanzia del libero esercizio del voto, dall'altro di garantire adeguatamente la validità della procedura legislativa. Il funzionamento del Parlamento italiano trova uno dei suoi principi fondanti nell'art. 64, terzo comma, Cost., il quale stabilisce che «le deliberazioni di ciascuna Camera e del Parlamento non sono valide se non è presente la maggioranza dei loro componenti, e se non sono adottate a maggioranza dei presenti, salvo che la Costituzione prescriva una maggioranza speciale». La previsione del numero legale ai fini della validità delle deliberazioni fornisce una specifica garanzia alle minoranze, mentre la richiesta che le deliberazioni siano adottate a maggioranza dei presenti – salvo che la Costituzione prescriva maggioranze speciali – costituzionalizza il principio maggioritario. Il concetto appare strettamente correlato a quello di "riunione" e sembra pertanto postulare la compresenza fisica

27. Reg. Camera 18 febbraio 1971 (1). Regolamento della Camera dei Deputati 18 febbraio 1971 (2). (1) Pubblicato nella Gazz. Uff. 1° marzo 1971, n. 53, S.O. (2) Approvato dall'Assemblea il 18 febbraio 1971.

28. Clementi 2020.

dei parlamentari; coerentemente, del resto, con la disciplina costituzionale della libertà di riunione (art. 17 Cost.), che si declina appunto come diritto a realizzare la compresenza, l'aggregazione in uno stesso luogo di una pluralità di persone. Il dovere di partecipare alle sedute (art. 1, comma 2, R.S.; art. 48-*bis* R.C.) va letto in stretta correlazione con altre disposizioni che prevedono esplicitamente o implicitamente la presenza fisica quale condizione per la partecipazione e lo svolgimento di determinate funzioni[29]. Disposizione che non avrebbe senso alcuno se fosse possibile partecipare alla seduta – e soprattutto alle votazioni – da uno spazio esterno[30].

In secondo luogo, è da evidenziare come il voto degli italiani all'estero avviene oggi con modalità analogiche che presentano numerose problematiche in tema di sicurezza, eppure nessuno obietta alcunché. Secondo la normativa generale, per quanto riguarda il voto degli italiani all'estero la legge n. 459/2001 stabilisce che i cittadini italiani residenti all'estero, iscritti all'AIRE, votano, per corrispondenza, nella circoscrizione Estero, per l'elezione delle Camere e per i referendum previsti dagli articoli 75 e 138 della Costituzione (art. 1). L'articolo 12 prevede al comma 6 che «Una volta espresso il proprio voto sulla scheda elettorale, l'elettore introduce nell'apposita busta la scheda o le schede elettorali, sigilla la busta, la introduce nella busta affrancata unitamente al tagliando staccato dal certificato elettorale comprovante l'esercizio del diritto di voto e la spedisce non oltre il decimo giorno precedente la data stabilita per le votazioni in Italia. Le schede e le buste che le contengono non devono recare alcun segno di riconoscimento».

In un simile procedimento non v'è alcuna possibilità di verifica che l'elettore sia solo e che esprima liberamente la propria votazione. Né la legge né il relativo manuale elettorale precisano le modalità di spedizione postale, in alcun modo prevedendo un sistema di tracciabilità.

Da ultimo, richiamando l'iniziativa di Cappato e della sua lista Democrazia e Referendum in materia di raccolta delle sottoscrizioni per la presentazione delle liste elettorali, è da evidenziare come allo stato attuale in Italia sia possibile (peraltro sempre per la meritoria iniziativa di Cappato) raccogliere sottoscrizioni digitali per la presentazione di referendum, mentre tale possibilità è inspiegabilmente preclusa per la raccolta delle firme necessarie alla presentazione delle liste elettorali in occasione delle elezioni politiche.

Una sottoscrizione digitale andrebbe inevitabilmente a rafforzare quelle liste non radicate sull'intero territorio nazionale, per le quali una raccolta firme in presenza (che, va ricordato, richiede la disponibilità di un soggetto abilitato ad autenticare le stesse) potrebbe risultare parecchio difficoltosa. A tale considerazione di natura pratico-operativa, se ne aggiunga la seguente. La raccolta delle sottoscrizioni per i referendum e le leggi popolari trova maggior favore da parte del legislatore in considerazione anche del carattere maggiormente tecnico e dei filtri più incisivi che la legge prevede. Quanto al referendum, a titolo esemplificativo, anzitutto è prevista una soglia molto più alta di sottoscrizioni, ben 500.000. A ciò si aggiunga la complessità tecnica imposta da un referendum di natura abrogativa, che dunque impone una corretta formulazione del quesito, tale da passare il rigido vaglio della Corte di Cassazione, chiamata ad esprimersi sull'ammissibilità stessa del referendum. A ciò si aggiunga ulteriormente il quorum richiesto. Ugualmente le leggi di iniziativa popolare, per quanto richiedano un numero di firme decisamente inferiore rispetto al referendum, esigono un elevato tecnicismo quanto alla loro predisposizione, oltre a prevedere un articolato iter per il loro esame (fase questa che peraltro sfugge al controllo dell'elettore). Prevedere dunque la possibilità di ricorrere alle sottoscrizioni digitali per referendum e leggi popolari rappresenta dunque una agevolazione rispetto a un iter di per sé già abbastanza complicato.

29. Si pensi, ad esempio, agli art. 2 e 3 R.S. e R.C. che fanno esplicito riferimento ai parlamentari presenti alla seduta; all'art. 6, comma 2, R.S. e R.C., ove la presenza di cinque senatori o sette deputati è posta come condizione di validità per le operazioni di scrutinio finalizzate all'elezione dell'Ufficio di Presidenza; all'art. 107 R.S., in materia di "Maggioranza nelle deliberazioni, numero legale ed accertamento del numero dei presenti", che va letto in connessione sistematica con il successivo art. 114, il quale prevede in caso di controprova la previa chiusura delle porte di accesso all'Aula.

30. Scaccia-Cariboni 2020.

7. Voto elettronico, democrazia e fiducia

Le elezioni sono l'espressione autentica della volontà degli individui e in quanto tali necessitano dunque di una procedura complessa. Tale procedura si articola nei seguenti passaggi: i) delimitazione dei collegi elettorali e degli aventi diritto al voto in ciascun collegio; ii) identificazione dell'elettore al momento del voto; iii) esercizio materiale della scelta tramite compilazione della scheda elettorale e successivo inserimento nell'urna; iv) scrutinio pubblico dei risultati e proclamazione dell'esito finale. Il voto è in qualche misura il racconto della democrazia e per essere esercitato in maniera adeguata abbisogna di procedure organizzate. Il dibattito sulle procedure di voto e sul sistema elettorale è storicamente un tema delicato data la intima connessione tra elezioni e potere: il voto tocca, infatti, direttamente le dinamiche del potere, in un certo senso ne regola e determina la legittimazione, ed è essenzialmente per queste ragioni che estenderne il diritto o modificarne le modalità ha comportato, sin dai tempi antichi, scontri di non poco conto[31].

Il voto elettronico rende evidenti distorsioni insite nella democrazia già presenti ben prima dell'avvento di forme di democrazia digitale che hanno ampliato il tema della sicurezza e del controllo sulle operazioni di voto. A ben guardare, già prima dell'avvento della democrazia digitale, il tema della legalità delle operazioni di voto e della sicurezza del voto era emerso a seguito di quello che sempre Lucio Pegoraro nel già richiamato contributo ha definito un surplus di informazioni imputabile al maggior flusso globalizzato rispetto ad anni fa[32]. Ugualmente, nota Marco Schirippa, i timori connessi all'avvento della democrazia digitale, per quanto logici e legittimi, non sono affatto differenti da quelli riscontrati in altre epoche a fronte delle precedenti rivoluzioni tecnologiche.

I detrattori del voto elettronico, appellandosi a sostegno delle proprie tesi all'argomento della sicurezza del voto, commettono un errore nella misura in cui ignorano un aspetto essenziale di qualsivoglia sistema democratico, ossia l'esistenza all'interno del sistema stesso di strumenti di controllo sulle votazioni e la presenza di rimedi a eventuali brogli che rappresentano una componente inevitabile all'interno del sistema democratico. Il controllo neutrale dei risultati elettorali rappresenta un fattore essenziale per la legittimazione democratica dei governi e delle loro maggioranze parlamentari.

Nel sistema democratico il consenso elettorale si regge sull'opinione pubblica e il fatto che questa possa percepire un difetto di trasparenza nei procedimenti elettivi comporta un corto circuito nel rapporto tra rappresentanti e rappresentati. Si delinea dunque la necessità di procedure elettorali caratterizzate da estrema trasparenza e passibili di controllo.

8. Riforme istituzionali, riforma del sistema elettorale e partecipazione democratica

I fautori del voto elettronico tendono spesso a giustificarne la necessità, tra i vari argomenti, facendo leva sul contrasto all'astensionismo e sull'allargamento della platea degli elettori. In una intervista rilasciata nel 2018, l'allora vice Presidente del Parlamento europeo Fabio Massimo Castaldo, dopo che il Parlamento UE ha dato il via libera alla possibilità dell'e-vote in vista delle europee del 2019, ha dichiarato che il voto elettronico potrebbe rappresentare sicuramente un volano per riavvicinare i cittadini alla politica, specie i giovani, molto vicini al mondo dell'innovazione ma lontani dal dibattito politico. Senza voler smorzare l'entusiasmo, si rendono al riguardo necessarie alcune precisazioni.

La prima ovvia precisazione è che tali affermazioni possono eventualmente valere con riguardo unicamente alle procedure di i-voting che, come s'è visto, implicano un ripensamento globale dei meccanismi di partecipazione democratica. Nulla cambierebbe con l'e-voting che, al contrario, si baserebbe sulle tradizionali procedure e che presuppone la necessità che il cittadino si rechi fisicamente al seggio elettorale nel giorno di votazione.

La seconda precisazione è che l'i-voting potrebbe rappresentare uno strumento di allargamento della platea elettorale ma non certo di contrasto all'astensionismo.

31. Schirripa 2021.

32. Tra i tanti casi all'attenzione delle cronache si consideri il celebre Bush vs Gore negli Stati Uniti. Sempre gli Stati Uniti, recentemente, hanno portato all'attenzione mediatica il caso dei presunti brogli denunciati dal Presidente uscente Donald Trump.

L'i-voting deve essere visto non tanto come uno strumento per abbattere/ridurre la disaffezione del cittadino verso la politica quanto piuttosto come uno strumento per abbattere le barriere che precludono l'esercizio del diritto di voto, il che è ben diverso. Sul punto, citando Gianmarco Gometz, la tesi delle virtù inclusive e partecipative del voto elettronico è allo stato carente di prove: proprio il caso dell'Estonia[33], sostiene lo studioso, consente di affermare che, pur a fronte di un leggero aumento dei tassi di *turnout*, non sussistono evidenze sufficienti a dimostrare che ciò sia dovuto al sistema di voto elettronico[34].

In ogni caso, ritengo, sempre condividendo le riflessioni di Gianmarco Gometz, che l'applicazione delle tecnologie digitali ai processi democratici del mondo reale, per sé, non assicura né impedisce che la democrazia funzioni meglio di quanto abbia fatto finora, non corregge né peggiora le storture eventualmente derivanti da un difettoso assetto istituzionale, non produce necessariamente soluzioni più condivise né è in grado di annullare i rischi di involuzioni antidemocratiche autoritarie. Soprattutto, la digitalizzazione della democrazia non ne altera il senso complessivo di impresa collettiva funzionale alla decisione per via maggioritaria su questioni controverse e irresolubilmente conflittuali, né la trasforma magicamente in una procedura produttiva di soluzioni "migliori" in quanto ponderate, ragionate o produttive di consenso sul "bene comune" o l'interesse generale[35].

Ciò del resto non sorprende; le tecniche della democrazia, in quanto tali, non cambiano la teoria della democrazia, i cui problemi come vedremo continuano a essere gli stessi di sempre anche nei nuovi scenari digitali.

Occorre però riconoscere che le tecnologie informatiche possono diventare un elemento importante del sostrato materiale di quel metodo di decisione collettiva che chiamiamo "democrazia", nel senso che possono agevolarne in vari modi l'esercizio e forse perfino influenzarne i risultati.

33. L'esperienza estone, in particolare, rappresenta uno delle più famose applicazioni dell'internet voting. In questo caso il voto elettronico, disponibile per chiunque, fa affidamento su un forte sistema di identificazione nazionale. Il sistema si basa sull'utilizzo di un documento di identificazione personale (ID card), legalmente accettato per l'identificazione tramite internet e per la firma digitale. Va infatti tenuto sempre a mente che presupposto indispensabile per qualsiasi sistema di i-voting è costituito da un sistema di autenticazione che garantisca nel modo più sicuro possibile l'identità del votante, atteso che viene a mancare il momento del riconoscimento al seggio elettorale. Gli elettori in possesso di ID card abilitata possono votare durante il periodo di advance voting (da 6 a 4 giorni prima della votazione): ciò permette agli elettori di cambiare il proprio voto, anche attraverso il voto cartaceo espresso nei seggi elettorali, per cui è, in ogni caso, stabilita una prevalenza nei confronti del voto elettronico (si parla a tal proposito di sistemi di voto a "doppio binario"). Per votare tramite internet è necessario il possesso di un lettore di smart card: l'elettore dopo essersi collegato al sito valimised.ee dovrà digitare il primo pin associato alla tessera. Il voto viene cifrato e l'utente deve digitare il secondo pin associato alla smart card; successivamente viene inviato all'Internet Server dove avviene il controllo di corrispondenza tra la firma e il proprietario della sessione (cioè se chi ha votato coincide con la stessa persona che ha iniziato il processo). L'Internet Server poi, in caso positivo, manda il voto cifrato al Vote storage server, che richiede un controllo sulla validità del certificato dell'elettore inviato dal Certificate server. Se valido, l'Internet Server verifica la firma digitale usando la chiave pubblica dell'elettore dal certificato dell'elettore. Alla fine del processo di voto l'elettore riceve sul monitor una conferma del fatto che il voto è stato espresso e correttamente registrato. Il voto resta nel server fino al momento del conteggio e tabulazione il giorno dell'elezione. Il successo di tale esperienza debba essere ricondotto ad una serie di precondizioni favorevoli, anzitutto di matrice territoriale. In effetti, l'Estonia si caratterizza per una minore densità abitativa rispetto all'Italia (pari a circa un milione di abitanti), che di certo ne ha favorito l'impiego generalizzato, su scala nazionale. In ogni caso, il successo del doppio binario concerne l'impiego del voto elettronico come "mezzo", risultando di converso inidoneo ad assolvere una funzione partecipativa, non avendo apportato alcun significativo incremento del numero dei votanti L'Estonia parte da condizioni diverse rispetto a noi in termini di cultura e consapevolezza digitale. problema di diffusione a tutti i livelli della cultura digitale.

34. Gometz 2017.

35. Gometz 2014.

Ad ogni buon conto, tornando all'esperienza italiana, affinché il voto elettronico possa trovare piena legittimazione nel sistema italiano il primo ostacolo da rimuovere è il digital divide (e quindi dell'accesso a Internet), che mette in crisi il requisito dell'universalità del voto.

Tale fenomeno taglia fuori quella parte importante dell'elettorato che non può avvalersi del voto elettronico a causa di almeno tre motivi: 1) abita in una zona non adeguatamente coperta dalla rete internet (si pensi alle molte zone di montagna); 2) è sprovvista dei mezzi tecnologici necessari e non può procurarseli a causa delle condizioni di povertà in cui versa; 3) è priva di una "cultura digitale" (o "informatica"), necessaria per saper utilizzare tali strumenti (questo, in particolare, accade per gli anziani o per i disagiati). A quest'ultimo riguardo, sebbene di dimensioni più ridotte rispetto al passato, quello dell'"analfabetismo digitale" appare essere un problema tutt'altro che superato, rendendosi particolarmente necessarie vere e proprie iniziative di "alfabetizzazione" nell'ottica di una maggiore inclusione dei cittadini.

9. Considerazioni finali

La ricostruzione sin qui effettuata, peraltro prendendo in esame anche casi concreti di brogli elettorali o comunque di criticità riscontrate in relazione ai più diversi sistemi di voto, permette di ritenere eccessivamente infondate le preoccupazioni dei detrattori del voto elettronico che può trovare legittimo spazio purché nell'ambito di procedure trasparenti e verificabili. Le preoccupazioni per la sicurezza celano una differente preoccupazione, che è quella per la tenuta del sistema democratico con i suoi riti e liturgie: in questo senso, il voto elettronico è potenzialmente in grado di determinare lo smarrimento del valore simbolico del voto, snaturando un processo altrimenti riflessivo e cancellando l'importanza dell'atto collettivo che si sta compiendo[36]. Eppure, la storia dei sistemi di voto si caratterizza da sempre per una costante ricerca del giusto equilibrio tra quattro elementi: trasparenza e pubblicità, da un lato (in riferimento in particolare alla procedura elettorale), segretezza e anonimato dall'altro (in riferimento alle modalità di espressione del voto da parte del cittadino). Partendo da questa consapevolezza, unitamente alla consapevolezza che i sistemi di sicurezza richiedono un costante intervento di monitoraggio e implementazione, ritengo si possa dare piena legittimazione al voto elettronico. In tal senso, del resto, si è già espressa a Commissione europea per la democrazia attraverso il diritto, istituita nel 1990, e meglio nota come Commissione di Venezia, dal nome della città in cui si riunisce. In particolare merita in questa sede di essere richiamato il contenuto del documento denominato *Report on the comparability of remote voting and electronic voting with the standards of the Council of Europe*. Secondo il testo del Codice di buona condotta in materia elettorale, ai fini di una reale democrazia occorre la compresenza dei 5 principi del patrimonio elettorale europeo, individuati nel suffragio (i) universale, (ii) uguale, (iii) libero, (iv) segreto, (v) diretto: in buona sostanza ogni elezione deve sempre assicurare la credibilità, attendibilità e trasparenza del processo elettorale. Il codice di buona condotta contiene una specifica sezione dedicata al voto meccanico e voto elettronico.

La nuova modalità di voto viene vista come possibile portatrice di vantaggi manifesti, purché si adottino le necessarie precauzioni al fine di limitare i rischi di frode. Il voto elettronico dunque dovrà essere sicuro e affidabile, garantire la riservatezza del voto, permettere verifiche e riconteggi in caso di reclamo, evitare ogni confusione nelle procedure di voto.

Riferimenti bibliografici

L. Caporusso (2008), *Elezioni come procedura. Forma, osservazione e automatizzazione del voto*, in "Italian Journal of Electoral Studies", vol. 59, 2008, n. 1

F. Clementi (2020), *Proteggere la democrazia rappresentativa tramite il voto elettronico: problemi, esperienze e prospettive (anche nel tempo del coronavirus). Una prima introduzione*, in "Federalismi.it", 2020, n. 6

36. Rosini 2021.

E. Colzani (2023), *Sottoscrizioni digitali in ambito elettorale: argomenti giuridici a favore*, in "Forum di Quaderni Costituzionali", 2023, n. 1

E. Colzani (2022), *Tre ostacoli al voto elettronico in Italia: pregiudizi, contraddizioni del sistema, carenza di cultura digitale*, in "Ciberspazio e Diritto", 2022, n. 3

T.E. Frosini (2021), *Prefazione*, in M. Schirippa, "Le nuove frontiere del diritto di voto. Uno studio di diritto comparato", Cedam, 2021

G. Gometz (2017), *Democrazie elettronica. Teoria e tecnica*, Ets edizioni, 2017

G. Gometz (2014), *Sulla "democrazia liquida". La segretezza del voto tra autonomia politica e bene comune*, in "Stato, Chiese e pluralismo confessionale", 2014, n. 30

M. Ladu (2023), *Contrastare l'astensionismo e favorire la partecipazione: il voto elettronico basato sulle tecnologie Blockchain e Distributed Ledger*, in "Media Laws", 2023, n. 1

G. Maestri (2020), *La democrazia e il segreto del voto, tra Italia e Stati Uniti Considerazioni a partire da un recente volume di Mimma Rospi*, in "Osservatorio Costituzionale AIC", 2020, n. 5

G. Nevola (2007), *Il malessere della democrazia contemporanea e la sfida dell'incantesimo democratico*, in "Il Politico", 2007, n. 1

L. Pegoraro (2011), *Problematiche attuali e prospettive di sviluppo del controllo sulle elezioni*, p. 352, in L. Pegoraro, G. Pavani, S. Pennicino (a cura di), "Chi controlla le elezioni? Verifica parlamentare dei poteri, tribunali, commissioni indipendenti", Bononia University Press, 2011

C. Pinelli (1996), *"Non sai che il voto è segreto?" L'affermazione di un principio costituzionale e delle sue garanzie*, in "Il Politico", 1996, n. 1

A. Ramos Tavares (2011), *La crisi della legittimazione elettorale*, in L. Pegoraro, G. Pavani, S. Pennicino (a cura di), "Chi controlla le elezioni? Verifica parlamentare dei poteri, tribunali, commissioni indipendenti", Bononia University Press, 2011

M. Rosini (2021), *Il voto elettronico tra standard europei e principi costituzionali. Prime riflessioni sulle difficoltà di implementazione dell'e-voting nell'ordinamento costituzionale italiano*, in "Rivista Associazione Italiana dei Costituzionalisti", 2021, n. 1

A. Sarais (2008), *Democrazia e tecnologie. Il voto elettronico*, Edizioni Esculapio, 2008

G. Scaccia, A. Cariboni (2020), *Funzionalità del Parlamento e modalità di voto nell'emergenza*, in "Forum di Quaderni Costituzionali", 2020, n. 3

M. Schirripa (2021), *Le nuove frontiere del diritto di voto. Uno studio di diritto comparato*, Cedam, 2021

S. Trancossi (2020), *Il paradossale ruolo della tecnologia nelle elezioni degli Stati Uniti*, in "Federalismi.it", 2020, n. 6

R. Zurita Aldeguer (2001), *Le influenze del sistema elettorale sulla costruzione della democrazia*, Contemporanea, 2001, n. 4

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0126 • articolo non sottoposto a peer review • pubblicato in anteprima il 12 gen. 2024

Simone Calzolaio

Isolamento e relazioni sociali. Il *Connection-in-All-Policies approach*

Nota a: U.S. Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023

Commento all'avviso del Surgeon General degli Stati Uniti relativo alle relazioni sociali – la loro struttura, funzione e qualità –, che rappresentano un contributo fondamentale e non sufficientemente considerato alla salute individuale e collettiva, alla sicurezza, resilienza e prosperità della comunità.

Relazioni sociali – Individui e comunità – Intelligenza artificiale

Isolation and social connection. The Connection-in-All-Policies approach

Commentary on: U.S. Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023

Commentary on the U.S. Surgeon General advisory focusing on Social connection – the structure, function, and quality of our relationships with others – as a critical and underappreciated contributor to individual and population health, community safety, resilience, and prosperity.

Social connection – Individuals and communities – Artificial intelligence

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

Il documento *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community* è disponibile nel sito dell'*Office of the Surgeon General* e all'indirizzo https://www.rivistaitalianadiinformaticaediritto/Social-Connection.pdf

1. Il *U.S. Surgeon General* e i suoi Rapporti e Pubblicazioni

Letteralmente, *U.S. Surgeon General* significa "chirurgo generale degli Stati Uniti".

Per chi si affaccia da lontano ad osservare l'ordinamento del servizio della salute pubblica statunitense si tratta di una istituzione singolare, che tuttavia si inquadra in modo coerente con la evoluzione storica della società e delle istituzioni americane[1], in forza della quale il chirurgo e il servizio sanitario della marina statunitense hanno seguito un processo di radicamento e istituzionalizzazione fino a divenire, dalla fine dell'Ottocento, rispettivamente il servizio della salute pubblica e il chirurgo generale degli Stati Uniti[2], con il suo apparato burocratico.

L'ufficio del Surgeon General è organizzato secondo le direttive e in accordo con il ministro della salute statunitense (U.S. Code, title 42, par. 203). Il Surgeon General è una figura istituzionale competente e carismatica: nominato dal Presidente degli Stati Uniti sentito il parere del Senato, resta in carica quattro anni[3], viene scelto fra i membri regolari dei *commissioned corps*, e deve possedere una formazione specializzata o un'esperienza significativa nei programmi di sanità pubblica.

Le attribuzioni di funzioni al cd. "dottore della Nazione", nel corso degli anni, sono variate sensibilmente, ma in sostanza, oltre ad essere il responsabile dei *U.S. Public Health Service Commissioned Corps* (USPHSCC), si occupa di indirizzare e sensibilizzare la popolazione americana e le politiche pubbliche verso abitudini di vita sane e salutari sulla base delle più aggiornate evidenze scientifiche[4]: questa attività viene svolta attraverso la pubblicazione di rapporti e di studi[5], elaborati col supporto della comunità scientifica e medica

1. Per una introduzione alla figura istituzionale, cfr. la pagina dedicata alla sua storia nel sito del U.S. Department of Health and Human Services.
2. Joel-Kaulback-Koenig et al. (2021), pp. 1758-1762.
3. Cfr., per indicazioni più specifiche, U.S. Code, title 42, par. 205.
4. Va sottolineato che l'ufficio del Surgeon General e l'ufficio del servizio di sanità pubblica statunitense curano la pubblicazione a partire dal 1878, con cadenza bimestrale, della Rivista scientifica *Public Health Reports*.
5. Cfr. https://www.hhs.gov/surgeongeneral/reports-and-publications/index.html.

statunitense, suddivisi in tre categorie: i Report[6], gli inviti all'azione[7], gli avvisi[8].

2. Perché rilevano i due *Advisories* del 2023

In alcuni ambiti, la pubblicazione di rapporti da parte del Surgeon General[9] ha esercitato una forte influenza e modificato, anche radicalmente, la sensibilità della popolazione e della politica americana e, di riverbero, mondiale: uno di questi ambiti è stato il fumo e la dipendenza da tabacco, in cui il *Report on Smoking and Health* del 1964[10] ha indubbiamente favorito la diffusione presso l'opinione pubblica di una consapevolezza condivisa sulla nocività del fumo e quindi favorito l'avvento di politiche restrittive sul fumo e di contrasto alla dipendenza da tabacco[11].

Per quanto qui interessa, sono due i profili da sottolineare in chiave introduttiva.

Il primo: come in precedenza osservato, negli Stati Uniti esiste una peculiare autorità competente in materia di salute pubblica che elabora rapporti e pubblicazioni documentate e autorevoli sulle tematiche più rilevanti e attuali di carattere sanitario, medico e socio-sanitario.

Il secondo: spesso questi rapporti hanno rivelato l'esistenza di fenomeni rilevanti per la salute pubblica, ancora non avvertiti come tali nella società, e hanno contribuito in modo rilevante, o perfino decisivo, a rendere consapevole l'opinione pubblica sui rischi, sulle cautele e sulle azioni da intraprendere per proteggersi da malattie, da fenomeni nocivi per la salute o da dipendenze, finendo con l'influenzare la progressiva adozione di politiche pubbliche e di azioni politiche su tali materie, negli Stati Uniti e spesso in larga parte del mondo.

Appare quindi notevole osservare che il Surgeon General, negli unici due *Advisories* pubblicati nel 2023[12], si sia concentrato su due tematiche a loro modo peculiari e innovative, offrendo evidenze epidemiologiche, descrizioni dell'evoluzione socio-sanitaria e suggerimenti in merito alle politiche da adottare che coinvolgono le conseguenze dell'avvento dell'ecosistema digitale e, specificamente, le attività delle compagnie tecnologiche, che come noto rappresentano un ganglio vitale dell'economia (e della supremazia) statunitense (nel mondo).

L'interesse che in questa sede è ragionevole nutrire per queste pubblicazioni deriva dalla potenziale analogia che può intuirsi sussistere fra il Report sugli effetti sulla salute del fumo del 1964 e questi due Avvisi del 2023: il Report del 1964 ebbe indubbiamente il merito di cristallizzare in un rapporto ufficiale di carattere scientifico ed epidemiologico quanto molti, all'interno della società e soprattutto nel mondo medico e scientifico, ormai ritenevano certo (la nocività del vizio del fumo) e che pure faticava non poco ad affermarsi in modo generale e in specifiche politiche pubbliche,

6. *Surgeon General's Reports*: documenti condivisi e revisionati dalla comunità scientifica, preparati da esperti incaricati da parte del Surgeon General, che rappresentano il punto di riferimento delle conoscenze scientifiche su un determinato tema, come, ad es,. la tematica delle dipendenze da alcol e droga.
7. *Surgeon General's Calls to Action*: documenti sintetici, scientificamente basati e fondati, che intendono richiamare l'attenzione su un tema rilevante e spesso preoccupante che investe la salute dei cittadini statunitensi, come, ad es., il tema dei suicidi, dell'ipertensione ecc.
8. *Surgeon General's Advisories*: si tratta di pubblicazioni che intendono richiamare l'attenzione su tematiche che rappresentano una sfida per la salute pubblica, individuando anche suggerimenti su come affrontarle.
9. Cfr. la pagina del sito del Surgeon General dedicata a *Reports and Publications*.
10. Cfr. *The 1964 Report on Smoking and Health*.
11. Cfr. Marshall 2014, pp. 250-278, e dottrina *ivi* citata (cfr. nota 3), ove si evidenzia proprio l'influenza del Report nella "istituzionalizzazione" dell'evidenza – allora tutt'altro che pacifica – della nocività del vizio del fumo. Recenti studi hanno evidenziato anche i limiti e contestualmente l'innovazione metodologica, per gli studi epidemiologici, di questo Report: cfr. Hall 2022, pp. 3170-3175.
12. Questi i due Advisories del 2023: 1) *Our Epidemic of Loneliness and Isolation. The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, del 3 maggio 2023; 2) *Social Media and Youth Mental Health*, del 23 maggio 2023; entrambi reperibili in *National Library of Medicine – Publications and Reports of the Surgeon General*.

complice anche il fatto che la ricchissima industria del tabacco era ed è un'industria prevalentemente a stelle e strisce. Il Report del 1964 fu una leva poderosa in tal senso ed anche un affatto scontato o prevedibile atto di indipendenza dell'apparato di salute pubblica americano da consolidati e pervasivi interessi economici[13].

Questi due avvisi del 2023 sembrano in qualche modo poter ricalcare quella dinamica: tutti percepiamo – in modo ancora indefinito, ora come allora – che l'avvento del digitale ha cambiato radicalmente il nostro modo di essere, prima ancora che di vivere, e che comporta rischi rilevanti per la tenuta delle relazioni personali, professionali, sociali, quindi, a cascata, per gli ordinamenti giuridici e, in particolare, per gli ordinamenti liberaldemocratici – che hanno bisogno del concorso responsabile delle persone e del popolo, per (r)esistere.

Tuttavia non siamo ancora in grado di descrivere compiutamente il fenomeno in corso, non abbiamo ancora una visione e un sapere affidabili su cosa sta accadendo e, finora, non abbiamo avuto evidenze specifiche – appunto: epidemiologiche – cui far riferimento per fondare e, soprattutto, per indirizzare correttamente la pur avvertita esigenza di regolazione delle tecnologie digitali per tutelare la vita sociale dopo la pandemia e nel nuovo – ma ormai consolidato – ambiente digitale.

Gli Avvisi del 2023 offrono un primo, documentato, punto di riferimento in tal senso.

3. Solitudine, isolamento e relazioni sociali: effetti sulla salute e sulla comunità

Our Epidemic of Loneliness and Isolation è un avviso suddiviso in 4 capitoli.

Nel primo capitolo si offre una visione di insieme del tema della "connessione sociale" – che credo noi tradurremmo con "relazioni sociali" – e delle ragioni per cui è così importante: ci si chiede cosa sia e come possa essere definita[14] (pp. 10-12), quale sia il suo andamento e se sia in declino (pp. 12-16), che cosa incide sul suo andamento e cosa ci spinge ad essere più o meno legati socialmente, anche con riguardo all'esperienza di isolamento collettivo derivante dalla pandemia da Covid-19 (pp. 16-22).

Obiettivo dichiarato dell'avviso è richiamare l'attenzione sul ruolo fondamentale[15] svolto dalle relazioni sociali sulla salute e sul benessere individuale e collettivo e offrire un quadro e un piano di azione per contribuire a promuovere le relazioni sociali: ciò in quanto la qualità delle relazioni sociali ha una incidenza diretta e documentata sulla salute e sulla aspettativa di vita, quindi sul sistema sanitario[16] e, contemporaneamente, le relazioni sociali sono in documentato declino e in crisi negli Stati Uniti – i dati del rapporto al riguardo sono tanto terribili quanto interessantissimi[17] e per di più legati ad un tema che forse è di maggiore attualità in Italia rispetto agli Stati Uniti: l'andamento demografico[18].

13. Cfr. Hall 2022.
14. Nel glossario iniziale, p. 7, si definisce "Social connection" come «A continuum of the size and diversity of one's social network and roles, the functions these relationships serve, and their positive or negative qualities" e "social disconnection" come "Objective or subjective deficits in social connection, including deficits in relationships and roles, their functions, and/or quality».
15. … sugli *healing effects*, cioè proprio sugli "effetti curativi", delle relazioni sociali e della comunità.
16. Infatti: «The lack of social connection poses a significant risk for individual health and longevity. Loneliness and social isolation increase the risk for premature death by 26% and 29% respectively. More broadly, lacking social connection can increase the risk for premature death as much as smoking up to 15 cigarettes a day. In addition, poor or insufficient social connection is associated with increased risk of disease, including a 29% increased risk of heart disease and a 32% increased risk of stroke. Furthermore, it is associated with increased risk for anxiety, depression, and dementia. Additionally, the lack of social connection may increase susceptibility to viruses and respiratory illness».
17. Si veda in particolare la tabella a p. 14, ove si documenta che la solitudine e l'isolamento crescono sia nel territorio di riferimento, sia nell'ambiente familiare, sia al di fuori delle famiglie.
18. Cfr. p. 15.

Il secondo capitolo dell'avviso documenta puntualmente come le relazioni sociali impattano sulla salute e il benessere individuale[19].

In primo luogo, vi sono evidenze scientifiche numerose, specifiche e convergenti sul fatto che le relazioni sociali impattano sulla salute individuale e, soprattutto, che la carenza di relazioni sociali diminuisce la speranza di vita e aumenta il rischio delle seguenti patologie: malattie cardiovascolari, ipertensione, diabete, malattie infettive (in particolare a causa della più debole risposta del sistema immunitario, ivi compreso nel caso di infezione da Covid-19), declino delle funzioni cognitive (solitudine e isolamento aumentano del 50% il rischio di sviluppare forme di demenza), depressione e ansia, tendenze suicide o autolesioniste (cfr. pp. 26-29). Rinviando all'avviso per più specifiche indicazioni – ma si veda la chiarissima tabella di p. 25 – si deve puntualizzare che non si tratta di "tendenze sociologiche", ma di evidenze epidemiologiche, cioè di statistiche vere e proprie sull'incidenza di malattie e sulla mortalità in caso di isolamento sociale e solitudine esistenziale.

In secondo luogo, una volta messa nero su bianco l'incidenza delle relazioni sociali sulla salute, ci si concentra sul tentare di comprendere come il nostro grado di relazioni sociali si riverberi ultimamente su una migliore o peggiore salute: secondo l'avviso, le relazioni sociali influenzano immediatamente i processi comportamentali, biologici e psicologici, i quali – interagendo sistematicamente fra loro – a loro volta influenzano lo stato di salute (cfr. pp. 32-34).

Infine, l'avviso documenta che buone relazioni sociali con i propri pari, con i genitori e con i docenti producono benefici non solo sul piano della salute individuale, ma anche e specificamente a livello formativo (*i.e.*, risultati scolastici e accademici) e a livello economico (impiego lavorativo, reddito).

Come si osserva nell'avviso, pertanto, i vantaggi della "connessione sociale" vanno oltre gli esiti legati alla salute ed influenzano il livello di istruzione, la soddisfazione sul posto di lavoro, la situazione economica e sentimenti generali di benessere e di pienezza di vita.

Queste conclusioni conducono al terzo capitolo, nel quale l'avviso indaga come le connessioni sociali impattano le comunità: «higher levels of social connectedness suggest better community outcomes, ranging from population health to community safety, resilience, prosperity, and representative government»[20].

Con il termine "comunità" ci si riferisce a un gruppo di persone che condivide una posizione geografica: (comunità del/la) quartiere, paese, città. Non solo: la connessione sociale delle comunità si riferisce alla comunità di persone presenti fisicamente (*in person*) l'una alle altre e non alle cd. comunità online o a distanza (p. 37).

Il passaggio è significativo, poiché lega le relazioni sociali (individuali) al benessere della comunità, coinvolgendo i concetti di capitale sociale, coesione sociale, supporto – diremmo noi, solidarietà – sociale, implicando le diverse tipologie di fiducia (generalizzata nel prossimo, individuale, nelle istituzioni) e costruendo le infrastrutture sociali su cui si basa la solidità (o la fragilità) delle società contemporanee e della società americana in particolare (pp. 37-38).

Le comunità attraversate da più intense relazioni sociali hanno maggiori benefici (pp. 39 ss.), misurabili, in tema di salute della popolazione, di capacità di prevenire e reagire di fronte a rischi di disastri ambientali o naturali, di sicurezza e ordine pubblico, di prosperità economica, di coinvolgimento civico e capacità di effettiva rappresentanza degli interessi da parte delle autorità di governo (grazie proprio alla diffusione più capillare dell'impegno civico nella comunità).

D'altra parte, le stesse relazioni sociali possono avere un lato negativo ed essere fonte di problemi, quando l'adesione ad un gruppo comporta la partecipazione a gang violente o a gruppi estremisti. Un rilievo specifico merita la polarizzazione sociale: cioè, la tendenza a instaurare relazioni sociali

19. … cfr. p. 23: «Numerose scoperte scientifiche provenienti da una varietà di discipline, tra cui l'epidemiologia, le neuroscienze, la medicina, la psicologia e la sociologia convergono verso la medesima conclusione: la connessione sociale è un predittore significativo della longevità e del miglioramento della salute fisica, cognitiva e mentale, mentre l'isolamento sociale e la solitudine sono significativi predittori di morte prematura e cattiva salute» [nostra traduzione].

20. … può sorprendere, ma c'è proprio scritto "governo rappresentativo".

solo con coloro che si ritengono più vicini a sé, escludendo o addirittura guardando con ostilità e sfiducia tutti "gli altri". Non a caso si cita l'esempio dei sentimenti di inimicizia e disapprovazione tra Democratici e Repubblicani sono più che raddoppiati tra il 1994 e il 2014 (p. 44) e, in questo modo, le relazioni sociali "polarizzate" impediscono un effettivo collegamento del capitale sociale (il cd. *bridging social capital*).

4. Investire nelle relazioni sociali: un compito pubblico, nella società digitalizzata post-pandemica?

L'avviso si conclude – cap. IV – proponendo una strategia nazionale per promuovere la connessione sociale.

L'*incipit* del capitolo enfatizza davvero il problema che l'avviso ha inteso affrontare, non in un tono moralizzatore, ma come una vera e propria emergenza nazionale: «The world is just beginning to recognize the vital importance of social connection. While the evidence of the severe consequences of social isolation, loneliness, and overall social disconnection has been building for decades, a global pandemic crystallized and accelerated the urgency for the United States to establish a National Strategy to Advance Social Connection. Such a strategy not only recognizes the critical importance of advancing social connection, but also serves as a commitment to invest in and take actions establishing that our connection with others is a core value of this Nation».

Sembra, onestamente, di essere tornati alle osservazioni ed ai timori manifestati e alle soluzioni ipotizzate ne *La Democrazia in America* da Tocqueville[21].

In ogni caso, la strategia si fonda su sei pilastri essenziali (1. rafforzare le infrastrutture sociali nelle comunità locali; 2. attuare politiche pubbliche a favore della connessione[22]; 3. mobilitare il settore sanitario; 4. riformare gli ambienti digitali: 5. approfondire la nostra conoscenza del fenomeno; 6. coltivare una cultura della connessione sociale) e su di una serie di raccomandazioni per gli stakeholder (p. 54 ss.).

Interessa soffermarsi qui su due profili, fra i molti.

Fa capolino, infatti, nello sviluppo dell'avviso un tema ricorrente: l'impatto del digitale sulle relazioni sociali e l'esigenza di riformare gli ambienti digitali.

Il tema dell'impatto delle tecnologie digitali sulle relazioni sociali resta sullo sfondo dell'avviso, viene centellinato in pochi sintetici passaggi ed evocato prudentemente, ma è altrettanto chiaramente implicato nel discorso sviluppato dal Surgeon General, il quale si domanda esplicitamente se l'ambiente digitale favorisca o renda più difficile la connessione sociale (pp. 19-21).

Accanto ai rilevanti benefici – quali mantenersi in contatto con le persone care, amici o familiari, o garantire una estesa e immediata possibilità di partecipazione sociale per tutti e in particolare per categorie altrimenti escluse, come i diversamente abili – emergono prepotentemente i profili dell'avvento del digitale che mutano radicalmente quantità e qualità delle nostre relazioni sociali: «several examples of harms include technology that displaces in-person engagement, monopolizes our attention, reduces the quality of our interactions, and even diminishes our self-esteem» (p. 20). Anche in questo ambito, l'avviso non è avaro di esempi e di dati, ormai consolidati, che conducono

21. … come noto egli riteneva che la (giovane) democrazia americana potesse correre il rischio di pervenire ad un governo dispotico, qualora fosse caduta nelle possibili degenerazioni del principio di eguaglianza, determinate in particolare dall'eccesso di individualismo, dalla conseguente spinta al conformismo sociale e, quindi, al giogo dispotico della tirannide della maggioranza: si vedano, volendo, il libro II, capp. VII-VIII (tirannide della maggioranza); il libro III, parte II, cap. II e ss. (individualismo); libro III, parte IV, cap. VI (quale dispotismo devono temere le nazioni democratiche), in de Tocqueville 2005. Non a caso, Tocqueville aveva individuato degli anticorpi nella democrazia americana, fra cui proprio il pluralismo sociale (libertà di associazione e libertà di stampa) e il pluralismo istituzionale (il federalismo e il ruolo delle comunità locali): si veda sul punto Barbera 2000, p. 25 ss., che davvero riconosce l'importanza della visione di Tocqueville nel contesto del costituzionalismo ottocentesco.

22. Interessantissimo il principio guida di questo pilastro: «Adopt a "Connection-in-All-Policies" approach», una sorta di principio della connessione sociale *by design*, applicato in tutte le politiche pubbliche.

a proporre la riforma degli ambienti digitali come azione-pilastro della strategia di promozione delle relazioni sociali.

Il Surgeon General affronta il discorso in modo decisamente maturo: non si tratta di esorcizzare l'ambiente digitale, ma di prendere atto dei cambiamenti che ha ormai strutturalmente indotto, di studiarli (in modo trasparente) e di adeguare le politiche in essere alle evidenze epidemiologiche ormai consolidate – e ci sono molti modi, e molto diversi fra loro, per farlo[23] – anche per identificare la distinzione fra le caratteristiche della connessione sociale digitale e, dall'altra parte, personale (p. 51).

In questo contesto emerge la funzione delle industrie tecnologiche, che hanno un triplice ruolo: garantire la trasparenza delle informazioni che mostrano gli impatti positivi e negativi della tecnologia sulle relazioni sociali; sostenere lo sviluppo e l'attuazione di standard di sicurezza in ambiente digitale; sviluppare tecnologie orientate al dialogo e alle relazioni sane, anche fra comunità e convinzioni fra loro diverse.

L'avviso pertanto sembra richiedere un investimento pubblico, di tipo istituzionale, regolatorio, promozionale, nelle sane relazioni sociali, nelle infrastrutture materiali e immateriali che favoriscono le sane relazioni sociali.

In qualche modo, si spiega in tal senso il titolo evocativo dell'avviso: è documentata una nuova, strisciante, epidemia nella società americana. L'epidemia della solitudine e dell'isolamento sociale, che provoca morte, malattie e violenza. Di fronte alle evidenze epidemiologiche che emergono nell'avviso, fra i compiti dell'Amministrazione americana e fra i valori fondanti degli Stati Uniti è ormai essenziale la promozione delle relazioni sociali e delle comunità di persone.

Ma come la si può sviluppare concretamente?

Il Surgeon General – e questo è il secondo profilo su cui ci si intende soffermare – dedica il secondo pilastro della sua strategia ad *Attuare politiche pubbliche a favore della connessione sociale* ed introduce il *"Connection-in-All-Policies" approach*: si tratta di un principio davvero interessante, in base al quale si richiede a tutti gli attori istituzionali (governo nazionale, statale, locale) di attivarsi in tutti i settori – perché tutti i settori sono rilevanti al fine di promuovere le relazioni sociali – cercando di identificare i fattori di connessione e disconnessione sociale, e ovviamente promuovendo i primi e combattendo i secondi attraverso politiche specifiche e con un monitoraggio trasversale. Non solo: questo approccio è *by design*, cioè si estende anche alle modalità con cui prodotti e servizi sono ideati, e devono essere ideati, tenendo conto dell'impatto sulle relazioni sociali[24].

Si tratta di un principio nuovo, quantomeno nella sua dimensione operativa, e sarà interessante verificarne eventuali applicazioni concrete, sia nelle politiche, sia nelle modalità di verifica del potenziale di disconnessione sociale implicato in prodotti e servizi, segnatamente in ambiente digitale.

5. L'intelligenza artificiale aiuta le relazioni sociali? Solidarietà, sussidiarietà, *Connection-in-All-Policies approach*

Non è necessario essere particolarmente esperto di storia e istituzioni americane per restare colpiti dal fatto che proprio dalla patria dell'individualismo e della tutela assoluta delle libertà individuali emerga un richiamo all'azione così forte e chiaro rivolto a promuovere una dimensione comunitaria e relazionale della società e una funzione promozionale e attiva dei poteri pubblici in tal senso.

In controluce si legge la preoccupazione viva per i fatti di Capitol Hill del 2021[25] e delle conseguenze del grande acceleratore dell'individualismo, dell'isolamento e della solitudine rappresentato – specialmente per le giovani generazioni – dall'avvento pervasivo delle tecnologie digitali, ma ormai, più correttamente, dell'ambiente digitale.

Ancor più, si intravede una preoccupazione per gli effetti ancora ignoti, ma potenzialmente ancor

23. … in molti si sono esercitati sul tema, ma di rilievo – specialmente per identificare l'approccio fra le due sponde dell'Atlantico – appare il contributo di Niro 2021.

24. … «A "Connection-in-All-Policies" approach recognizes that every sector of society is relevant to social connection, and that policy within each sector may potentially hinder or facilitate connection. Conversely, *government has a responsibility to use its authority to monitor and mitigate the public health harm caused by policies, products, and services that drive social disconnection*» (p. 49, nostro il corsivo).

25. Cfr. *Assalto a Capitol Hill, un'ombra sul futuro*, in ispionline.it.

più significativi, del «dislivello prometeico»[26] derivante dall'avvento dell'intelligenza artificiale.

Infatti, molti si preoccupano delle potenziali conseguenze catastrofiche dell'avvento dell'intelligenza artificiale: macchine di cui si perda il controllo e che improvvisamente, e autonomamente, provochino conseguenze irreparabili.

Credo tuttavia che l'importanza dell'Avviso sia anche nell'aiutare a porre attenzione ad un aspetto concreto e immediato implicato dall'avvento dei sistemi di IA nelle società contemporanee e, in particolare, sulle cd. liberaldemocrazie: l'intelligenza artificiale aumenta le connessioni sociali? Qual è l'impatto dell'IA – si pensi all'IA generativa – sulle relazioni sociali?

Di per sé – quale che sia la definizione da utilizzare, su cui in seno all'Ue ancora cortesemente ci si accapiglia[27] – un sistema di intelligenza artificiale agevola o sostituisce o aumenta la capacità dell'essere umano in attività che, in precedenza, doveva faticosamente svolgere da solo – e in riferimento alle quali quindi spesso si trovava in condizione di dover chiedere aiuto, cioè di dover instaurare una relazione sociale: qualcuno penserà immediatamente a ChatGpt, ma suggerirei invece di soffermarsi su Google Maps.

Se invece di acquistare cartine e mappe stradali e/o di rivolgersi a chi si ha intorno, c'è un sistema che trova immediatamente il percorso stradale migliore per giungere a destinazione, si è guadagnato molto tempo e risparmiata molta fatica. Come in concreto avvenuto in questi anni, il sistema di Google Maps è divenuto virale. Ciò ha comportato, tuttavia, che progressivamente sono venute meno, e strutturalmente, relazioni sociali e canali di relazioni sociali un tempo consolidati e normali, se non proprio inevitabili, come approvvigionarsi di cartine stradali e chiedere consigli prima e durante il percorso.

Cosa compensa questa perdita? Cosa compensa la strutturale perdita di esperienza e di competenza (nel conoscere le strade!) dell'essere umano? Quali rischi (sociali) corriamo a fronte di così evidenti benefici?

La risposta dell'Avviso è in qualche modo molto originale e inaspettata.

Non sappiamo cosa può compensare la tendenza epocale – accelerata dalle tecnologie digitali – verso l'individualismo e verso la difficoltà ad avere relazioni sociali sane (positive anche se imperfette, appassionate ma non violente, durature e non solo provvisorie, feconde e non sterili). Ma sappiano che negli Stati Uniti le istituzioni che si occupano della salute e del benessere pubblico documentano che il tema delle relazioni sociali e della loro solidità è legato alla salute e alla aspettativa di vita e, pertanto, richiedono un investimento regolatorio e politiche pubbliche di sostegno alla connessione sociale.

Riecheggia pertanto negli USA una rinnovata attualità del principio pluralista e del principio personalista, che la nostra Costituzione fa propri con la formula quasi poetica dell'art. 2 della Costituzione italiana: i doveri di solidarietà politica economica e sociale – che appaiono spesso un richiamo evanescente –, e la stessa logica del principio di sussidiarietà in senso orizzontale, si arricchiscono ora di un nuovo principio operativo, che fa anche da ponte all'evoluzione sociale e digitale della società statunitense e, prevedibilmente, della nostra: il *Connection-in-All-Policies approach* del Surgeon General statunitense. Questa nuova formula, questo nuovo compito dei poteri pubblici, è uno strumento in grado di diminuire l'inquietante ma sempre affascinante dislivello prometeico derivante dall'avvento delle nuove tecnologie e dell'IA? Vedremo. Ma il dato è tratto.

This research was funded by the European Union – NextGenerationEU under the Italian Ministry of University and Research (MIUR), National Innovation Ecosystem grant ECS00000041-VITALITY-CUP D83C22000710005

26. … di cui parla giustamente Luciani 2023.

27. … intanto negli Stati Uniti cfr. l'*Executive Order* n. 14110 del 30 ottobre 2023, su *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

Riferimenti bibliografici

A. Barbera (2000), *Le basi filosofiche del costituzionalismo*, Laterza, 2000

A. de Tocqueville, (2005), *La democrazia in America*, (a cura di) G. Candeloro, RCS libri, 2005

W. Hall (2022), *The 1964 US Surgeon General's report on smoking and health*, in "Addiction", vol. 117, 2022, n. 12

M.A. Joel, K. Kaulback, G.J. Koenig, C.J. Yeo, J.A. Marks (2021), *A brief history of the office of the Surgeon General and the 2 surgeons who have held the position*, in "Surgery", vol. 170, 2021, n. 6

M. Luciani (2023), *La sfida dell'intelligenza artificiale*, Lettera AIC 12/2023

T.R. Marshall (2014), *The 1964 Surgeon General's Report and Americans' Beliefs about Smoking*, in "Journal of the history of medicine and allied sciences", vol. 70, 2014, n. 2

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolamentazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0127 • articolo non sottoposto a peer review • pubblicato in anteprima il 12 gen. 2024

Simone Calzolaio

Social media e minori. Il *Safety-first approach*

Nota a: U.S. Surgeon General, *Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory*, 2023

Commento all'avviso del Surgeon General degli Stati Uniti che presenta un'analisi indipendente sull'impatto dei social media sui giovani proponendo le azioni che dovrebbero essere intraprese da policymaker, aziende tecnologiche, adulti e famiglie, e ricercatori.

Social media – Bambini e adolescenti – Benefici e danni dell'uso dei social media

Social media and youths. The Safety-first approach

Commentary on: U.S. Surgeon General, *Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory*, 2023

Commentary on the U.S. Surgeon General advisory presenting an independent analysis of the impact of social media on youth, proposing actions to be taken by policymakers, technology companies, parents and caregivers, and researchers.

Social media – Children and adolescents – Benefits and harms of social media use

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

Il documento *Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory* è disponibile nel sito dell'*Office of the Surgeon General* e all'indirizzo https://www.rivistaitalianadiinformaticaediritto.it/Youth-Mental-Health.pdf

1. Il U.S. Surgeon General e l'avviso sulla salute mentale dei giovani e social media

A pochi giorni dall'adozione dell'avviso concernente l'epidemia di solitudine e isolamento sociale, il Surgeon General ha adottato un ulteriore avviso, in tema di social media e salute mentale dei giovani[1].

Questo nuovo avviso è suddiviso in tre parti: una introduzione e l'individuazione degli effetti, positivi e negativi, dei social media sui bambini e sugli adolescenti (pp. 4-7); l'analisi delle evidenze scientifiche in merito ai danni derivanti dalla esposizione a contenuti nocivi o da uso eccessivo o problematico dei social media, oltre alla identificazione di una serie di domande specifiche in ordine alle quali vi è necessità di approfondimento scientifico e non vi sono ancora evidenze scientifiche conclamate (pp. 8-12); le azioni da intraprendere da parte dei soggetti coinvolti (pp. 13-19).

2. Così fan tutti. Impatto dei social sui giovani e fattori di rischio

Nell'avviso risultano chiari sin dall'inizio due dati.

Gli adolescenti sono sistematicamente e massivamente online: oltre il 95% dei giovani fra i 13 e i 17 anni utilizzano piattaforme social e, fra questi, una quota consistente è costantemente presente online. Come noto, l'età minima, formalmente richiesta, per l'utilizzo di queste piattaforme è di 13 anni e purtuttavia risulta che almeno il 40% dei bambini fra 8 e 12 anni utilizza i social media.

In questo contesto, sorge spontanea la domanda in ordine all'impatto che questa frequentazione sistematica dei social media ha sui giovani. L'avviso afferma chiaramente che sono necessarie ulteriori e specifiche ricerche per determinare in modo condiviso e generale tipologia ed entità di rischi o di danni derivanti dall'uso dei social media per i bambini e adolescenti. Quindi un impatto c'è, ed è documentabile, ma non in modo ancora sufficientemente nitido e chiaro, nei suoi profili determinanti: c'è ancora molta ricerca da svolgere.

Tuttavia, ormai un numero cospicuo di ricerche consente di individuare una connessione fra determinati fattori e i rischi di danno per la salute mentale dei giovani, come in particolare: il tempo complessivamente speso sui social media, il tipo di contenuti prodotti/utilizzati o a cui si è esposti, le attività/interazioni offerte dal social media, il grado di influenza negativa su attività essenziali come il sonno e l'attività fisica. Inoltre, le ricerche mostrano come l'impatto dell'uso dei social media sia differente a seconda della specifica condizione sociale o situazione di vulnerabilità in cui il minore si trova.

Un tema specifico attiene al rapporto fra utilizzo dei social media da parte dei giovani e sviluppo del cervello, in forza del quale risulta che

1. Oltre all'avviso che qui si commenta (Office of the Surgeon General (OSG) 2023a), si veda anche Office of the Surgeon General (OSG) 2023, commentato in Calzolaio 2023; entrambi sono reperibili anche all'indirizzo: https://www.ncbi.nlm.nih.gov/books/NBK45031/.

l'uso frequente dei social media può influenzare lo sviluppo della amigdala (importante per la sfera dell'apprendimento emotivo e del comportamento) e la corteccia prefrontale (importante per il controllo degli impulsi, la regolazione emotiva e la moderazione del comportamento sociale) e comportare una aumentata sensibilità alla disapprovazione o all'apprezzamento sociale.

L'uso dei social media è un fattore predittivo di una decrescita conseguente del livello di soddisfazione di vita, in particolare per le ragazze da 11 a 13 anni e per i ragazzi di 14/15 anni.

3. Benefici e danni dell'uso di social media

L'avviso (pp. 5-7) riporta anche degli effetti benefici derivanti dall'uso dei social media da parte dei minori, come l'espressione e la connessione di carattere comunitario, in particolare per le minoranze razziali, etniche, sessuali e di genere, che possono sentirsi maggiormente riconosciute e non discriminate proprio nell'ambiente dei social media. Inoltre, i social media possono essere un canale privilegiato per la richiesta di aiuto specialistico nell'ambito di problemi di benessere e salute mentale in genere.

Accanto a questi benefici, si apre lo scenario del ben più articolato ambito dei danni derivanti dall'uso di social media. In particolare, vengono riportati 4 aspetti:

1) è documentato che l'esposizione di adolescenti (12-15 anni) per più di 3 ore al giorno su social media ha effetti negativi sulla salute mentale, compresi sintomi di depressione e ansia;
2) uno studio molto articolato sugli studenti dell'ottavo e del decimo anno di scuola (corrispondenti all'incirca alla nostra terza media e secondo anno della scuola superiore) mostra che in media tali studenti passano circa 3,5 ore al giorno sui social media e che l'introduzione di una nuova piattaforma social è associata all'aumento di depressione (9%) e ansia (12%) rispetto alla situazione precedente;
3) sono documentati effetti diretti e positivi sulla (lotta alla) depressione di giovani e adulti, derivanti già dalla mera limitazione dell'uso di social media a 30 minuti al giorno per 3 settimane consecutive;
4) è documentato un problema specifico derivante dall'uso dei social media per le ragazze adolescenti, in particolare uno studio su ragazzi/e di 14 anni mostra che il maggior utilizzo dei social media conduce a disturbi del sonno, molestie online, immagine negativa del proprio corpo, bassa autostima, un aumento dei sintomi depressivi, più per le ragazze che per i ragazzi.

4. In particolare: danno da esposizione a contenuti e danno da uso eccessivo o problematico

L'avviso si concentra nel descrivere due specifiche tipologie di danno cui vanno soggetti bambini e adolescenti nella navigazione su social media (pp. 8-10).

Il primo profilo è il danno da esposizione a contenuti inappropriati, che si articola a sua volta in una molteplicità di fattispecie: contenuti che spingono alla emulazione violenta, all'autolesionismo e al suicidio; contenuti che, in modo sistematico, spingono ad una comparazione con gli altri e quindi inducono ad una visione negativa del proprio corpo, a disordini alimentari e finanche alla manifestazione di sintomi depressivi; ancora, l'esposizione a contenuti d'odio (discriminatori, violenti, molesti) ed alle relative conseguenze psico-emotive; infine, ipotesi di vero e proprio sfruttamento o adescamento di minori online da parte di malintenzionati, adulti o meno.

Accanto a questi danni, non meno rilevanti sono quelli derivanti da un uso eccessivo o problematico dei social media.

In quest'ambito, colpisce particolarmente che il primo effetto negativo dell'uso eccessivo dei social media è l'interruzione o l'ostacolo a comportamenti salutari, altrimenti ordinari e tradizionalmente assodati, di bambini e adolescenti: il modello "economico" dei social media per sua natura ha l'obiettivo di attrarre e massimizzare l'implicazione e il tempo trascorso dai ragazzi sui social, poiché questo fa aumentare i guadagni e l'influenza del social media. La parola d'ordine è *maximize engagement*[2]

2. Gli strumenti di cui si avvalgono i social media a tal fine sono, ad es., «push notifications, autoplay, infinite scroll, quantifying and displaying popularity (i.e., 'likes'), and algorithms that leverage user data to serve content recommendations» (p. 9).

e l'effetto sui giovani è sconfortante: l'avviso documenta che l'attaccamento ai social media ha effetti sul cervello paragonabili a quelli di altre dipendenze (da stupefacenti o dal gioco) e che oltre un terzo delle ragazze fra 11 e 15 anni dichiara di sentirsi dipendenti dai social media e oltre la metà degli adolescenti afferma che sarebbe arduo disconnettersi dai social media. Si tenga presente che studi credibili concernenti i ragazzi fra la terza media e il secondo superiore (italiani) affermano che il tempo medio trascorso sui social media è di 3,5 ore al giorno, mentre 1 giovane su 4 trascorre più di 5 ore al giorno e 1 su 7 trascorre più di 7 ore al giorno sui social media.

In questa situazione, è comprensibile il nesso fra un uso così sistematico e capillare dei social media e l'uso compulsivo o incontrollabile dei social, i problemi di sonno, di concentrazione e attenzione, i sentimenti di esclusione ed il loro sempre più spesso ingestibile impatto sugli adolescenti. Non è ancora definitivamente provato, ma sembra sussistere un nesso fra l'uso eccessivo dei social media e i disturbi di deficit di attenzione e dell'iperattività (*attention-deficit/hyperactivity disorder* – ADHD) negli adolescenti.

5. Le questioni aperte e da approfondire ancora

L'avviso si concentra anche nel definire quali sono le domande di ricerca ancora aperte e le esigenze di documentazione ancora inevase o incomplete ed è piuttosto crudo nel definire l'esigenza di ulteriori ricerche: «quasi tutti i teenager americani usano i social media e noi non abbiamo ancora abbastanza prove per concludere che si tratta di un ambiente sufficientemente sicuro per loro. I nostri bambini sono divenuti partecipanti inconsapevoli di un esperimento decennale. È vitale che ricercatori indipendenti e compagnie tecnologiche lavorino insieme per far avanzare rapidamente la nostra comprensione dell'impatto dei social media su bambini e adolescenti» (mia la traduzione, p. 11).

Di seguito le specifiche domande poste dal Surgeon General. Come si può facilmente intuire hanno davvero una portata universale e attuale, e possono perfino sembrare ingenue o eccessive, ma d'altra parte qualcuno doveva pur porle in un documento ufficiale di carattere medico-sanitario:

- In che modo le interazioni sociali di persona e quelle digitali differiscono in termini di impatto sulla salute e qual è l'influenza specifica del comportamento sui social media alla connessione sociale, all'isolamento sociale e ai sintomi della salute mentale?
- Quali sono i potenziali percorsi attraverso i quali i social media possono causare danni alla salute mentale e al benessere dei bambini e degli adolescenti? Per esempio: in che modo la comparazione sociale influisce sul senso di soddisfazione della vita e relazioni di persona? In che modo l'uso dei social media, inclusi design e funzionalità specifici, è correlato alle vie della dopamina coinvolte nella motivazione, nella ricompensa e nella dipendenza?
- Che tipo di contenuto, e con quale frequenza e intensità, genera il maggior danno? Attraverso quali modalità di accesso ai social media (ad es. smartphone, computer) e caratteristiche del design? Per quali utenti e perché?
- Quali sono gli effetti benefici dei social media? Per quali categorie si verificano i maggiori vantaggi? In quali modi e in quali circostanze?
- Quali fattori a livello individuale, comunitario e sociale possono proteggere i giovani dagli effetti negativi dei social media?
- Quali tipi di strategie e approcci sono efficaci nel proteggere la salute mentale e il benessere di bambini e adolescenti sui social media (ad esempio, programmi, politiche, caratteristiche di progettazione, interventi, norme)?
- In che modo l'uso dei social media interagisce con lo stadio di sviluppo di una persona per misurare il rischio di impatto sulla salute mentale?

Nessuno, in realtà, allo stato ha una risposta, o anche solo un inizio di risposta adeguata a queste domande. Per questo è bene riportarle integralmente e non censurarle, affinché si possa adeguatamente osservare e riflettere sul dislivello attualmente esistente fra l'esposizione dei giovani ai social media e il livello di sicurezza di queste piattaforme.

6. Cosa si può e si deve fare. Il *safety-first approach*

L'avviso afferma testualmente che negli Stati Uniti è in atto «una crisi nazionale di salute mentale giovanile» – testuale, p. 13, righe 9/10 – e che questa crisi è largamente causata anche dall'utilizzo da parte di bambini e adolescenti di piattaforme di social media pensate per gli adulti. Esiste pertanto

un problema concernente il modo con cui i social media sono attualmente progettati, distribuiti, utilizzati.

Al momento le famiglie sono l'unico presidio di tutela dei minori, ma non sono autosufficienti: il Surgeon General afferma che ci sono azioni che le aziende tecnologiche possono intraprendere per rendere le loro piattaforme più sicure per bambini e adolescenti; ci sono azioni che i ricercatori possono intraprendere per sviluppare la base di ricerca necessaria a supportare ulteriori garanzie e c'è un ruolo per la politica locale, statale e federale nell'implementare la protezione dei bambini e degli adolescenti.

E viene altresì richiamata la tradizione statunitense di *safety-first approach* anche in altri settori (pp. 13-14), per giustificare l'esigenza pressante di applicarlo al rapporto fra social media e minori.

Secondo l'avviso, spetta ai policymaker sviluppare diverse politiche in materia fra cui preme ricordarne qui due: standard di salute e sicurezza adeguati all'età per le piattaforme tecnologiche, che significa, in particolare, limitare le funzionalità e l'accesso in funzione e in ragione dell'età e dello sviluppo del minore; limitare gli strumenti catalizzatori dell'attenzione per i minori; aumentare lo standard di protezione dei dati personali dei minori; rafforzare ed estendere – effettivamente – le limitazioni di età all'accesso sui social media dei minori. Inoltre, spetta ancora ai policymaker vincolare le compagnie tecnologiche a condividere con ricercatori indipendenti i dati necessari a verificare l'impatto sulla salute delle loro piattaforme.

Le aziende tecnologiche hanno evidentemente un ruolo specifico nella protezione dei minori, in quanto progettano le piattaforme social. Fra i diversi aspetti indicati nell'avviso, ve ne sono tre centrali: trasparenza, collaborazione effettiva con ricercatori indipendenti, *health and safety by design* delle piattaforme social.

Ci sono anche dei compiti per i genitori e per gli adulti (*caregivers*): in particolare, avere un piano per l'utilizzo in famiglia dei media[3], creare delle zone franche dalla connessione e incoraggiare i minori a frequentarsi in presenza, essere di esempio nell'utilizzo dei media, collaborare con gli altri genitori e adulti per stabilire regole condivise sull'uso dei social media da parte dei ragazzi.

Spetta ai ragazzi – essenzialmente – comportarsi in modo avveduto e prudente (p. 18).

Una parte importante – cui in qualche modo si intende contribuire sin d'ora – spetta ai ricercatori: in modo particolare, è compito di chi sviluppa la ricerca riuscire ad individuare metriche condivise per la qualificazione e la valutazione dei rischi e dell'impatto dei social media sui minori. Su questo aspetto solo la ricerca libera può fornire, progressivamente, un quadro condiviso su cui, poi, policymaker e aziende possono agire, interagire, confliggere.

7. I due avvisi del 2023. Isolamento e salute mentale dei giovani: il fil rouge e quella strana libertà del Surgeon General

È abbastanza evidente che l'avviso qui commentato apre uno spaccato che è impensabile esaurire in poche battute.

Pertanto si vuole convogliare l'attenzione su due soli profili conclusivi.

In primo luogo, vi è un nesso evidente fra i due avvisi del 2023: l'epidemia di isolamento e solitudine (con i suoi effetti sulla aspettativa di vita e sulla salute) della popolazione statunitense è strettamente legata alla salute mentale dei giovani nell'ambiente digitale dei social media.

Ciascuno dei due avvisi richiama e richiede l'applicazione di un principio cardine in tutte le politiche pubbliche implicate: il primo avviso fa riferimento al *Connection-in-All-Policies approach*, il secondo avviso al *Safety-First approach*. È abbastanza evidente che i due approcci siano connessi, ma è altresì abbastanza chiaro – anche nello sviluppo dell'avviso qui in commento (cfr., ad es., p. 17) – che l'idea chiave su cui entrambi gli Avvisi si fondano è che la promozione sistematica delle relazioni sociali (a tu per tu!) sia l'unico antidoto, l'unica arma che le persone e le comunità possono sfruttare per limitare il pervasivo inaridimento cognitivo, e poi sociale, e poi istituzionale, che deriva dall'iper-connessione.

La base fattuale dei due Avvisi è rappresentata da pressanti ed evidenti rischi e danni socio-sanitari, che sono davvero puntualmente documentati in entrambi – l'apparato di riferimenti bibliografici è forse l'aspetto più prezioso di entrambi gli Avvisi.

3. … può essere preso alla leggera, ma si veda il *Family Media Plan* dell'American Academy of Pediatrics.

Sullo sfondo – e fra le righe – degli Avvisi del 2023 si legge tuttavia una diffusa preoccupazione sulla vulnerabilità e sulla capacità di tenuta del tessuto sociale della democrazia americana: adulti sempre più soli e giovani sempre più sotto il tallone dei social media possono costituire una base solida per una democrazia liberaldemocratica?

D'altra parte, non si può non rilevare che questi due Avvisi provengano proprio dall'ordinamento da cui forse era più improbabile attenderseli. Gli Stati Uniti sono la patria delle piattaforme social e di internet, da cui traggono buona parte della supremazia tecnologica che ne fa la prima potenza mondiale. Eppure ciò non impedisce che sia proprio un soggetto che dipende dal Governo degli Stati Uniti – il Surgeon General – a denunciare i danni alla salute dell'isolamento sociale e della solitudine accelerate, se non prodotte, dalle piattaforme digitali e l'esigenza di un cambiamento radicale nelle politiche statunitensi in materia sociale e digitale, per proteggere le relazioni sociali e la coscienza dei giovani. È indubbiamente una felice contraddizione, quella della democrazia statunitense che, ancora una volta, sarà bene studiare accuratamente, in Europa e in Italia.

This research was funded by the European Union – NextGenerationEU under the Italian Ministry of University and Research (MIUR), National Innovation Ecosystem grant ECS00000041-VITALITY-CUP D83C22000710005

Riferimenti bibliografici

S. Calzolaio (2023), *Isolamento e relazioni sociali. Il Connection-in-All-Policies-approach. Nota a: U.S. Surgeon General, Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community, 2023*, in "Rivista italiana di informatica e diritto", 2023, n. 2

Office of the Surgeon General (OSG) (2023), *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 3 May 2023

Office of the Surgeon General (OSG) (2023a), *Social Media and Youth Mental Health*, 2023

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0114 • articolo non sottoposto a peer review • pubblicato in anteprima il 18 ott. 2023

OSSERVATORIO SU

Intelligenza Artificiale e diritto

coordinato da Giancarlo Taddei Elmi

GIANCARLO TADDEI ELMI - SOFIA MARCHIAFAVA

Sviluppi recenti in tema di Intelligenza Artificiale e diritto

Una rassegna di legislazione, giurisprudenza e dottrina

giugno-agosto 2023

G. Taddei Elmi è ricercatore associato presso l'IGSG/CNR di Firenze. S. Marchiafava è avvocato cassazionista, LLM in Comparative Law, docente del Master di II livello in Informatica giuridica, nuove tecnologie e diritto dell'informatica presso Sapienza – Università di Roma

A. Normativa

1. Iter legislativo della proposta di legge sull'intelligenza artificiale - procedimento 2021/0106/COD

Prosegue la procedura legislativa ordinaria relativa alla *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, presentata dalla Commissione europea il 21 aprile 2021, COM(2021) 206.

In particolare, dopo l'Orientamento generale adottato dal Consiglio il 6 dicembre 2022, il Parlamento europeo ha espresso nella seduta plenaria del 14 giugno 2023 la sua posizione negoziale votando (499 voti a favore, 28 contrari e 93 astensioni) gli emendamenti introdotti al testo della proposta, P9_TA(2023)0236. Nel corso della conferenza stampa tenutasi immediatamente dopo la votazione la Presidente del Parlamento europeo Roberta Mětsola e i correlatori Brando Benifei (Commissione per il mercato interno e la protezione dei consumatori) e Dragoș Tudorache (Commissione per le libertà civili, la giustizia e gli affari interni) hanno illustrato alcuni dei punti principali del testo emendato.

Tra gli emendamenti approvati dal Parlamento europeo si segnalano quelli riguardanti:

- la definizione dei sistemi di IA, ampliata e con un richiamo alla necessità di allinearla «al lavoro delle organizzazioni internazionali che si occupano di IA»;
- l'alfabetizzazione in materia di IA;
- le pratiche vietate e il relativo elenco che è stato ampliato includendo tra i sistemi di IA da vietare: (a) i sistemi di identificazione biometrica sia per l'uso "in tempo reale" sia per quello "a posteriori"; (b) i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili (ad esempio, genere, razza, etnia, status di cittadinanza, religione, orientamento politico); (c) i sistemi di polizia predittiva (basati sulla profilazione, l'ubicazione o il comportamento criminale pregresso); (d) i sistemi di riconoscimento delle emozioni (utilizzati nell'ambito di attività di contrasto dalle forze dell'ordine, nella gestione delle frontiere, nei luoghi di lavoro e negli istituti di istruzione); (e) i sistemi di IA che utilizzano l'estrazione indiscriminata di dati biometrici dai social media o da filmati di telecamere a circuito chiuso per creare banche dati di riconoscimento facciale;
- la classificazione dei sistemi di IA ad alto rischio che deve includere anche quelli con un "rischio significativo" per la salute, la sicurezza, i diritti fondamentali o l'ambiente nonché i sistemi di IA utilizzati per influenzare gli elettori e impiegati nei sistemi di raccomandazione visualizzati dalle piattaforme online di dimensioni molto grandi;
- l'introduzione per i sistemi di IA ad alto rischio della valutazione d'impatto sui diritti fondamentali;
- l'obbligo di informare quando un sistema di IA ad alto rischio è impiegato per fornire assistenza in un processo decisionale o nel prendere decisioni relative a persone fisiche;
- i cosiddetti spazi di sperimentazione normativa, specificamente definiti, da istituire negli Stati membri (almeno uno) e da rendere diffusamente disponibili in tutta l'Unione europea e accessibili a PMI e startup;

– l'impulso della ricerca e dello sviluppo dell'IA a sostegno di risultati proficui in ambito sociale e ambientale;
– l'accesso significativo a meccanismi di segnalazione nel caso di violazione e il diritto di presentare ricorsi e reclami anche mediante un procedimento interno.

La posizione adottata in prima lettura dal Parlamento europeo è stata trasmessa al Consiglio e alla Commissione europea nonché ai parlamenti nazionali. Seguono i negoziati sul testo definitivo del regolamento che come auspicato dalle stesse istituzioni europee dovrebbe essere approvato entro la fine del corrente anno.

2. Protezione dei dati personali e IA

2.1. Unione europea

La regolamentazione dell'Unione europea sui dati ha una notevole rilevanza anche per l'adozione e lo sviluppo dell'IA come già sottolineato nella comunicazione della Commissione europea dal titolo *Una strategia europea per i dati* del 19 febbraio 2020, COM(2020) 66. In effetti, «la disponibilità di dati è essenziale per l'allenamento dei sistemi di intelligenza artificiale». Nell'ambito dell'attuale quadro normativo rivolto alla realizzazione nell'Unione europea di un mercato unico dei dati vanno indicate le seguenti recenti iniziative legislative.

a) Regolamento sulla governance dei dati (c.d. *Data Governance Act*)

Tenuto conto dello stretto legame tra i dati e l'IA va ricordato che a decorrere dal 24 settembre 2023 sarà applicabile il *Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724* (Regolamento sulla governance dei dati)

b) Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)

Il 28 giugno 2023 è stato raggiunto l'accordo politico tra il Parlamento europeo e il Consiglio sulla *Proposta di Regolamento del Parlamento europeo e del Consiglio dalla Commissione europea riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, presentata dalla Commissione il 23 febbraio 2022, COM(2022) 68. Tale accordo rappresenta una tappa fondamentale dell'iter legislativo in via di definizione.

2.2. Garante italiano per la protezione dei dati personali e ChatGPT

A seguito dei provvedimenti assunti a livello nazionale a protezione dei dati personali degli utenti in relazione a ChatGPT, illustrati nel precedente aggiornamento pubblicato da questo Osservatorio, OpenAI, società statunitense che sviluppa e gestisce l'applicazione in questione, ha comunicato le seguenti misure adottate in conformità a quanto chiesto dal Garante italiano per la protezione dei dati personali con il provvedimento dell'11 aprile 2023, in particolare:
– predisposizione e pubblicazione dell'informativa rivolta a tutti gli utenti e non utenti, nell'Unione europea e negli altri paesi extraeuropei, finalizzata a illustrare quali dati personali e con quali modalità sono trattati per l'addestramento degli algoritmi e per ricordare che chiunque ha diritto di opporsi a tale trattamento;
– ampliamento dell'informativa sul trattamento dei dati riservata agli utenti del servizio, ora accessibile anche nella maschera di registrazione prima che un utente si registri al servizio;
– riconoscimento a tutte le persone che vivono nell'Unione europea, anche non utenti, del diritto di opporsi a che i loro dati personali siano trattati per l'addestramento degli algoritmi anche attraverso un apposito modulo compilabile online e facilmente accessibile;

- predisposizione di una schermata di benvenuto alla riattivazione di ChatGPT in Italia, con rinvii alla nuova informativa sulla privacy e alle modalità di trattamento dei dati personali per il training degli algoritmi;
- possibilità per gli interessati di far cancellare le informazioni ritenute errate dichiarandosi, allo stato, tecnicamente impossibilitata a correggere gli errori;
- spiegazione, nell'informativa riservata agli utenti, che mentre continuerà a trattare taluni dati personali per garantire il corretto funzionamento del servizio sulla base del contratto, tratterà i loro dati personali ai fini dell'addestramento degli algoritmi, salvo che esercitino il diritto di opposizione, sulla base del legittimo interesse;
- predisposizione di un modulo che consente a tutti gli utenti europei di esercitare il diritto di opposizione al trattamento dei propri dati personali e di poter così escludere le conversazioni e la relativa cronologia dal training dei propri algoritmi;
- inserimento nella schermata di benvenuto riservata agli utenti italiani già registrati al servizio di un pulsante attraverso il quale, per accedere nuovamente al servizio, dovranno dichiarare di essere maggiorenni o ultra-tredicenni e, in questo caso, di avere il consenso dei genitori;
- inserimento nella maschera di registrazione al servizio della richiesta della data di nascita prevedendo un blocco alla registrazione per gli utenti infra-tredicenni e prevedendo, nell'ipotesi di utenti ultra-tredicenni non maggiorenni, che debbano confermare di avere il consenso dei genitori all'uso del servizio.

Il Garante italiano per la protezione dei dati personali ha espresso piena soddisfazione per l'introduzione delle suddette misure auspicando l'attuazione delle ulteriori prescrizioni stabilite dallo stesso provvedimento dell'11 aprile 2023: implementazione di un sistema di verifica dell'età, pianificazione e realizzazione di una campagna di comunicazione finalizzata a informare tutti i cittadini italiani della vicenda e della possibilità di opporsi all'utilizzo dei propri dati personali ai fini dell'addestramento degli algoritmi. L'attività istruttoria avviata nei confronti di OpenAI è ancora in corso, ma ChatGPT è nuovamente utilizzabile anche in Italia.

B. Giurisprudenza

Riservatezza - Trattamento dei dati contenuti nel certificato medico - Utilizzazione a fini antifrode del software "Data mining Savio" - Profilazione

Cass. civ., Sez. I, Ordinanza, 01 marzo 2023, n. 6177

> «In materia di protezione dei dati personali, pur rientrando nei diritti fondamentali della persona di cui all'art. 2 Cost., il diritto ad esigere una corretta gestione dei dati personali e particolari deve essere necessariamente coordinato e bilanciato con le disposizioni costituzionali che tutelano altri diritti come – per quanto ora rileva – l'interesse pubblico alla trasparenza, alla celerità e al buon andamento dell'attività amministrativa di cui all'art. 97 Cost.» (*Quotidiano Giuridico*, 2023).
>
> «In tema di trattamento dei dati personali contenuti nel certificato medico inviato dal dipendente per la liquidazione dell'indennità di malattia, l'I.N.P.S., nell'utilizzazione, ai fini antifrode, del software denominato "Data mining Savio" non viola il disposto dell'art. 14 del d.lgs. n. 196 del 2003 (nella versione "ratione temporis" applicabile): difettano, infatti, i requisiti della profilazione (in quanto il soggetto non viene mai individuato o inserito in una determinata categoria o profilo), del trattamento "unicamente" automatizzato (in quanto gli operatori effettuano ulteriori verifiche) e della valutazione di un "comportamento umano" (poiché la personalità dei singoli interessati non viene mai delineata dal sistema) (Cassa e decide nel merito, Tribunale di Roma, 03 marzo 2020)» (*CED Cassazione*, 2023). Per un primo commento, Viggiani 2023.

C. Dottrina

1. Saggi e volumi

L. Califano, *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati*, in "federalismi.it", 2023, n. 10, pp. IV-XV

Si esamina la questione della regolamentazione delle tecnologie digitali e del loro uso, con particolare riferimento all'IA e ai provvedimenti del Garante per la protezione dei dati personali in relazione al caso di ChatGPT e Meta EDI. Entrambi i casi, infatti, suscitano numerose riflessioni, dalla questione della tutela dei dati personali e di addestramento, ai contenuti presenti in rete. D'altra parte, il contesto tecnologico, caratterizzato da finalità in prevalenza commerciali, incide anche sulla formazione del consenso democratico, sull'esercizio delle libertà e del diritto di voto dei cittadini. In tale contesto, a tutela del pluralismo politico e informativo, è essenziale il GDPR, come peraltro emerge dalle decisioni del Comitato europeo per la protezione dei dati (EDPB) richiamate, nonché il quadro normativo europeo riguardante le piattaforme digitali e l'IA.

C. Caporale, L. Palazzani (a cura di), *Intelligenza Artificiale: distingue frequenter. Uno sguardo interdisciplinare*, Cnr Edizioni, 2023

Il volume affronta il tema dell'IA con uno sguardo interdisciplinare. Alla prefazione di Giuliano Amato e all'introduzione della curatrice Caporale seguono diversi contributi individuali che sul tema offrono una visione complessiva (P. Benanti, *Le stagioni dell'IA*; C. Collicelli, *Le scienze sociali di fronte all'IA*; E. Mazzarella, *Contro l'infosfera. Salvare la presenza*; L. Palazzani, *Cosa resta dell'umano nell'epoca dell'IA*; A. Raspanti, *Le domande della teologia cristiana sull'IA*; S. Zamagni, *IA ed etica pubblica*; L. Antonini, A. Sciarrone Alibrandi, *Alla ricerca di un Habeas Corpus per l'IA*; L. Becchetti, *La funzione degli algoritmi e il discernimento umano*; G.R. Gristina, L. Orsi, *L'IA: sostituzione o sostegno del medico?*; J.-P. Darnis, C.M. Polvani, *IA e umano: uno sguardo d'insieme*).

L. Floridi, *AI as Agency Without Intelligence: on ChatGPT, Large Language Models, and Other Generative Models*, in "Philosophy & Technology", March 2023

I "Large Language Models" (LLM), modelli di linguaggio di grandi dimensioni, come ad esempio tra i più noti GPT3, ChatGPT o GPT3.5 (OpenAI-Microsoft), Bard (Google) e LLaMA (Meta), sono incapaci di pensare, ragionare e capire, ma la crescita e quantità di dati a disposizione, la velocità di calcolo, la qualità degli algoritmi, consentono loro di ottenere ottimi risultati, analoghi a quelli dei processi intellettuali umani. A tale premessa segue la descrizione di alcuni casi pratici con abilità e limiti di questi modelli che operano su basi statistiche senza comprendere il significato dei testi. In ogni caso le implicazioni dei contenuti generati dai LLM e dai sistemi di IA saranno assai rilevanti come si chiarifica riferendosi al caso di DALL-E, sistema di IA che trasforma testi in immagini, sviluppato da OpenAI. Tra le molteplici questioni (etiche, giuridiche, sociali, economiche, ecc.) sussiste anche il problema dell'uso di tali strumenti tenuto conto degli ulteriori sviluppi tecnologici e dell'interazione tra e con questi sistemi che sebbene privi di intelligenza sono dotati di autonomia e capacità di apprendimento inediti.

N.A. Kissinger, E. Schmidt, D. Huttenlocher, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, Mondadori, 2023

Viene posta una serie di interrogativi evidenziando i benefici e rischi dell'IA, la possibile alterazione dell'identità umana e percezione della realtà, la trasformazione dell'esperienza per effetto dell'utilizzazione crescente dei sistemi di IA, per esempio per la ricerca e l'informazione. Nel ripercorrere gli sviluppi

dell'IA si sottolineano l'interazione sempre più stretta tra intelligenza umana e artificiale, la velocità dei cambiamenti, l'importanza del ruolo dell'IA anche per le piattaforme di rete globali e l'ordine internazionale offrendo al lettore una panoramica e diversi autorevoli spunti di riflessione.

N. Lucchi, *ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems*, in "European Journal of Risk Regulation", June 12, 2023, pp. 1-23

Le questioni del diritto d'autore e dei sistemi di IA generativa sono trattate con particolare riguardo al caso di ChatGPT. Per generare risultati di qualità i sistemi di IA generativa richiedono quantità sostanziali di dati di addestramento che spesso riguardano informazioni protette dal diritto d'autore. Occorre riflettere sui principi legali del "fair use", sulla creazione di opere derivate e sulla liceità della raccolta e dell'utilizzo dei dati. L'utilizzo dei dati allo scopo di addestrare e migliorare i modelli di IA suscita notevoli preoccupazioni riguardo a potenziali violazioni del diritto d'autore. A proposito di possibili soluzioni, attraverso l'analisi dell'applicazione ChatGPT, ci si sofferma sulle modifiche da introdurre alle normative sul diritto d'autore per poter affrontare adeguatamente le complessità della paternità e della proprietà dei contenuti creativi generati dall'IA.

F. Pizzetti, *Con AI Verso la Società digitale*, in "federalismi.it", 2023, n. 23, pp. IV-IXX

L'evoluzione della società digitale è fondata sui dati e i loro trattamenti. Il ricorso alle tecnologie di IA basate sulla Data Analytics consente trattamenti sempre più ampi di dati e analisi sempre più sofisticate con trasformazioni sociali epocali. Di qui l'importanza di regole che rendano tra l'altro verificabili e sindacabili i dati usati per l'addestramento di queste tecnologie e per la loro attività di analisi. In tale contesto il GDPR (Regolamento generale sulla protezione dei dati personali) ha svolto un ruolo precursore.

2. Nota: Ancora sulla Soggettività dei Sistemi di Intelligenza Artificiale

Commento a margine degli emendamenti del Parlamento europeo approvati il 14 giugno 2023 (P9_TA(2023)0236) alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione

La questione Soggettività dei SIA va impostata sotto due aspetti: a) come Soggettività ontologica "riconosciuta" in base al possesso di requisiti essenziali quali la percezione-sensazione "sentita", la immaginazione-fantasia, la intellezione "semantica" e non solo morfo-sintattica, la autocoscienza e la autodeterminazione "voluta"e b) come Soggettività ascritticia "conferita" dall'ordinamento in base a criteri di opportunità e utilità pratico-funzionali.

Sin dai lontani anni Novanta del secolo scorso ci siamo interrogati se i sistemi di IA iperintelligenti superassero la soglia della dicotomia cosa-persona e potessero essere tutelati anche secondo soggettività e non solo per valore[1]. La risposta all'epoca non poteva che essere negativa. I sistemi di allora erano totalmente etero-predeterminati a priori e non presentavano alcun livello di autonomia per cui era impossibile parlare di forme di soggettività ontologiche sia pure ridotte. Si cominciava però a ventilare l'ipotesi di personalità giuridica attribuita al fine di superare problemi di responsabilità per atti illeciti prodotti dai SIA.

La dottrina nel corso degli anni Novanta e nel primo decennio del 2000 si mostra divisa tra i fautori di tale possibilità e i nettamente contrari o almeno molto scettici. La prepotente evoluzione dei SIA verso

1 Taddei Elmi 1990.

tecnologie self-learning, che consentono una autonomia sempre più spinta, nel secondo decennio del 2000, costringe a riproporre il dilemma cosa-persona.

Nel frattempo anche l'Europa finalmente scopre l'Intelligenza artificiale come possibile strumento di azioni produttive di illeciti non facilmente inquadrabili nelle categorie tradizionali della responsabilità. Si moltiplicano le lacune normative non agevolmente risolvibili con interpretazione e analogia.

Accanto al suggerimento di utilizzare le categorie della responsabilità oggettive e indirette il Parlamento europeo in una ormai famosa Risoluzione del 2017 avanza per i SIA molto autonomi l'ipotesi della attribuzione di uno status di *electronic person*. A seguito di questa idea, "indecente" per molti, si scatena di nuovo il dibattito tra favorevoli e contrari alla personalità giuridica del SIA.

Attraverso vari studi e documenti l'Europa critica come inutile e inopportuna l'ipotesi della persona giuridica dei SIA, per arrivare alla sua bocciatura definitiva nella Risoluzione del PE dell'ottobre del 2020 dove si propone la emanazione di un regolamento del Parlamento europeo e del Consiglio che stabilisce regole sulla responsabilità per il funzionamento dei sistemi di IA.

Distingue tra SIA ad alto rischio per i quali propone le figure tradizionali delle responsabilità oggettive e indirette e i SIA non ad alto rischio dove ritiene applicabile la responsabilità per colpa.

Nell'aprile 2021 la Commissione europea presenta una proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.

Tale proposta non menziona assolutamente ipotesi di personalità giuridica e, seguendo un approccio basato sul rischio, distingue tra pratiche inaccettabili vietate, pratiche ad alto rischio e pratiche a basso o minimo rischio, non esprimendosi sui conseguenti aspetti della responsabilità. Il silenzio pare far propria l'indicazione della Risoluzione del Parlamento Europeo dell'ottobre del 2020 che, nella allegata proposta di Regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, raccomanda l'adozione di quella oggettiva per i SIA ad alto rischio e di quella per colpa per tutti gli altri.

Il 14 giugno 2023, successivamente alla posizione comune adottata il 6 dicembre 2022 dal Consiglio riguardo alla suddetta proposta normativa sull'IA, il Parlamento europeo in seduta plenaria approva gli emendamenti al testo della proposta del 2021 dove continua a non rilevarsi alcun richiamo a ipotesi di personalità giuridica dei SIA.

D'altra parte le ipotesi di soggettività ontologiche (ossia consapevoli) più o meno piene sembrano oggi ancora lontane malgrado il crescente sviluppo tecnologico. I SIA c.d. neurali operano in stato di totale inconsapevolezza; si autodeterminano ma non si rendono conto di autodeterminarsi.

De iure condendo si potrebbe immaginare un riconoscimento del SIA inconsapevoli alla stregua dei soggetti cerebralmente disabili totali.

Resta ancora in piedi l'interrogativo di *quando* i SIA potrebbero superare la soglia della inconsapevolezza e diventare in qualche misura coscienti.

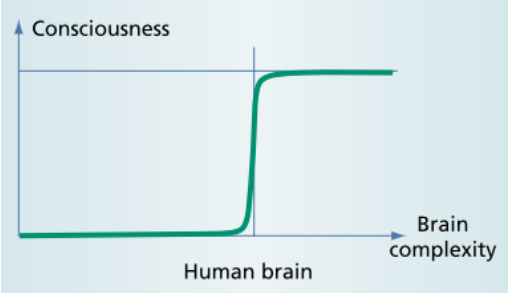
Il cruciale problema dei soggetti ontologici dipende dalla costruzione di un cervello artificiale identico al cervello biologico ossia un artefatto non solo intelligente ma cosciente.

Secondo l'IA forte la coscienza è un prodotto del cervello e dipende dalla quantità di neuroni e di connessioni sinaptiche attivate contemporaneamente; sarebbe una questione di quantità e non di qualità.

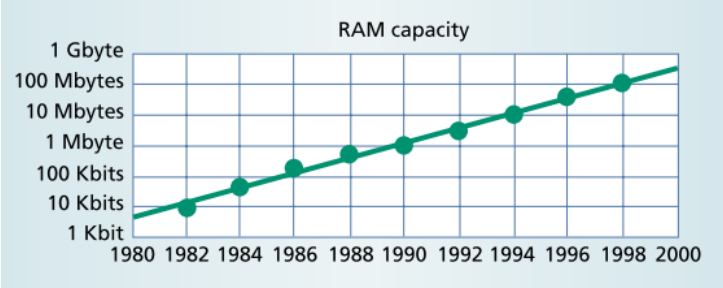
In un articolo risalente Giorgio Buttazzo[2] ventilava un'ipotesi fantagiuridica e fantascientifica basata sul rapporto tra coscienza e complessità cerebrale. Il cervello possiede circa mille miliardi di neuroni e ciascuno di essi sviluppa mediamente mille connessioni sinaptiche con gli altri neuroni per un totale di dieci alla quindicesima.

La tendenza delle dimensioni della RAM dei calcolatori è approssimabile secondo la seguente formula sulla base dello sviluppo tecnologico degli ultimi venti anni.

2. Buttazzo 2002.



Rapporto tra coscienza e complessità cerebrale



Tendenza tecnologica. La RAM della coscienza

Sulla base della tendenza di cui al grafico precedente si presume che una disponibilità di RAM di 1015 (connessioni neuronali) si raggiungerà nel 2029.

Se questa ipotesi, che lega strettamente la coscienza alla quantità di connessioni elettriche, risultasse vera bisognerebbe rivisitare tutte le nostre conclusioni sul superamento della dicotomia cosa-persona. L'IA cosciente risponderebbe personalmente delle proprie azioni!?[3]

A tale scenario si possono avanzare immediatamente obiezioni pregiudiziali e scientifiche.

Obiezione logica pregiudiziale: possedere una RAM di dieci alla quindicesima sarebbe condizione in ogni caso necessaria ma non sufficiente per concludere che quel cervello elettronico possiede stati di coscienza.

Obiezione scientifica: il funzionamento del cervello biologico pare non consistere solo in connessioni neuronali elettriche, ma potrebbe dipendere anche da fenomeni bio-chimici e fisici come l'energia prodotta da vibrazioni quantiche dei microtuboli cerebrali (Teoria *Orch-or*[4]) e da vibrazioni elettromagnetiche sempre prodotte dai neuroni[5].

Posto dunque che un SIA con soggettività ontologica piena o ridotta non pare all'orizzonte della scienza e della tecnologia, una linea da seguire forse potrebbe essere quella verso una soggettività *sui generis*, un *tertium genus*[6], da attribuire o riconoscere ai SIA in quanto tali. Così come si riconosce agli animali o ad altre entità più o meno fisiche, a entità bioniche (*cyborg*) e a entità dotate di intelligenza "sovrumana", senza indagare troppo sui loro stati interni di consapevolezza o inconsapevolezza.

3. Per un'ampia riflessione scientifica-filosofica-giuridica ed etica sull'intelligenza artificiale (2017-2018) vedi in generale i contributi in *Atti e memorie dell'Accademia toscana di scienze e lettere La Colombaria*, vol. LXXXII, n.s. LXVIII, Leo S. Olschki, 2017 e in particolare, sul passaggio da intelligenti a coscienti, vedi Taddei Elmi 2017.
4. Hameroff-Penrose 2014.
5. Mc Fadden 2020.
6. Mayinger 2017.

Si tratterebbe di entità intermedie sempre inconsapevoli ma titolari di diritti e doveri quali il diritto di esistere e il dovere di non procurare danno, pena lo spegnimento o disattivazione provvisoria o definitiva. Si tratterebbe di una soggettività artificiale collocata tra soggettività naturale o ontologica e soggettività giuridica o ascritticia, dotata di capacità di agire secondo regole prestabilite dall'ordinamento.

Giancarlo Taddei Elmi

D. Eventi, seminari, convegni, notizie

Pluralismo e diritto d'autore al tempo dell'intelligenza artificiale, Roma, 21 settembre 2023, convegno organizzato da Agcom (Autorità garante per le garanzie nelle comunicazioni) in collaborazione con il Chapter italiano IIC (International Institute of Communications)

A partire dai saluti istituzionali dei presidenti dell'Agcom, Giacomo Lasorella, e del Chapter italiano IIC, Augusto Preta, è stato illustrato l'impatto dell'IA sul pluralismo e diritto d'autore, sottolineando il significativo numero di utenti e il problema della lingua dei dati di addestramento, prevalentemente la lingua inglese (Erik Lambert, Chapter Italiano IIC). Le opportunità e i rischi dell'IA generativa vanno affrontate con un approccio interdisciplinare (Giuseppe F. Italiano, Università Luiss Guido Carli), le relative problematiche giuridiche sono inedite (Marco Bassini, Università di Tilburg, Paesi Bassi) e il compito del diritto appare assai complesso e rischia di essere vanificato dalla velocità degli sviluppi tecnologici (Francesco Posteraro, Avvocato, già commissario dell'Agcom). Nell'ambito della discussione del ruolo delle Istituzioni europee e delle Autorità nazionali è stato in particolare esaminato quello dell'Agcom (Massimiliano Capitanio, Commissario Agcom) e dell'Autorità garante per la protezione dei dati personali, basti pensare ai recenti provvedimenti assunti in relazione al caso di ChatGPT (Ginevra Cerrina Feroni, Vice-presidente del Garante per la protezione dei dati personali). All'annuncio di un tavolo su IA e mondo dell'editoria e informazione (Alberto Barachini, Sottosegretario di Stato alla Presidenza del Consiglio dei ministri), è seguita una analisi delle implicazioni della c.d. eccezione di Text and Data Mining (TDM) della direttiva (UE) 2019/790, c.d. direttiva copyright, (Giuseppe Abbamonte, Direttore Media Policy DG Connect). Sul ruolo delle imprese sono intervenuti Alessandra Santacroce (Direttore relazioni istituzionali, IBM Italia), Andrea Stazi (Regulatory Affairs Regional Lead, Google) e Antongiulio Lombardi (Direttore affari regolamentari, WindTre) che in conclusione ha prospettato due soluzioni già oggetto di analisi da parte delle Istituzioni europee: il riconoscimento della personalità elettronica ai sistemi di IA e l'assicurazione obbligatoria.

Governo e scienza dell'acqua. Sfida per intelligenze umana, naturale, artificiale, Roma, 18 luglio 2023

La tavola rotonda è stata organizzata dalla XII Commissione, Affari Sociali e Sanità, della Camera dei deputati. La relazione introduttiva di Ugo Ruffolo ha inquadrato il problema dell'acqua e delle acque rispettivamente come bene e come regime osservando che in origine il governo delle acque spettava all'intelligenza naturale e umana, mentre a seguito degli sviluppi dell'IA e delle sue applicazioni la gestione potrebbe essere affidata a sistemi di IA per garantire maggiore efficienza. Sono seguiti gli interventi programmati. Cesare Pinelli, nel ricordare la ripartizione delle competenze tra Stato e Regioni, ha sottolineato anche la dimensione sovranazionale e internazionale delle questioni relative all'acqua. Maurizio Gabrielli si è trattenuto sull'impatto favorevole della transizione digitale nel governo dell'acqua, soprattutto con riferimento ai sistemi di supporto alle decisioni ovvero a strumenti che a partire dai dati possono aiutare il processo decisionale. Tali sistemi si articolano secondo quattro componenti: 1) analisi dei dati, 2) diagnosi dei dati, 3) predizione basata sull'analisi e sulla diagnosi dei dati, 4) prescrizione (il sistema può dire cosa si deve fare). Seguendo tale sistema si passa dalla visione della diga alla ragione dell'esondazione; sull'esperienza passata si riesce a predire con metodi statistici il modello prescrittivo che dice cosa si deve fare. Attualmente, tali sistemi devono avere un controllo umano. Gabrielli ha poi

segnalato l'importanza del Digital Twin: sistema basato su modelli matematici che consente di effettuare delle sperimentazioni, Il Centro europeo per le previsioni meteorologiche a medio termine di Bologna ha l'obiettivo di realizzare un gemello digitale del pianeta. Del pari i modelli matematici per le acque sono fattibili; si possono creare modelli dai consumi per ottimizzare ed evitare gli sprechi. Un esempio è quello dei consumi maggiori che avvengono in agricoltura; con l'agricoltura di precisione è possibile sviluppare modelli diagnostici predittivi per effettuare irrigazioni più razionali riducendo i consumi. Nei disastri esistono dei modelli predittivi, modelli di supporto alle decisioni. Sistemi per il controllo della qualità delle acque attraverso modelli predittivi che per esempio indicano i rischi di contaminazione, i sistemi possono monitorare l'acqua e la qualità.

Sui modelli diagnostici, predittivi e di supporto alla decisione si è anche soffermato Giovanni Sartor ponendosi l'interrogativo delle conseguenze nel caso di risposta inadeguata dei modelli stessi rispetto all'obiettivo per il quale sono stati realizzati. Se falliscono o conducono a risultati inadeguati? Se c'è un difetto nella predizione? È possibile parlare di negligenza? Sartor ha poi rimarcato l'importanza dell'attività di simulazione e modellazione delle dinamiche ambientali, in particolare la possibilità di realizzare dei gemelli per verificare, anticipare le questioni della gestione delle acque. Successivamente sono intervenuti Franco Cotana sul ruolo fondamentale dell'acqua per la transizione energetica e Andrea Amidei che dopo aver accennato all'importanza dell'impiego dell'IA nella sanità (settore in forte crescita) si è soffermato sull'acqua come diritto e presupposto per la tutela di altri diritti (per esempio, proprio quello alla salute). L'IA può portare un significativo contributo nella gestione della risorsa dell'acqua sempre più scarsa. Secondo Amidei potrebbero quindi sorgere nuovi standard esigibili da parte della PA e il suo buon andamento (artt. 97 e 98 cost.). Se la PA non contempla gli strumenti tecnologici di questo tipo è conforme agli artt. 97 e 98 cost.? I sistemi di IA come strumenti fondamentali sono tutti idonei a gestire questa fondamentale risorsa? Quale potrebbe essere il potenziale impatto dell'utilizzo dei sistemi di IA? Quali i requisiti? Amidei ha ricordato l'importanza della regolazione, per esempio quella che nell'Unione europea è in via di definizione che prevede sistemi di IA per la gestione di risorse critiche, sistemi di IA menzionati tra quelli ad alto rischio. Altrettanto rilevanti sono gli standard, il controllo e monitoraggio dei sistemi di IA. Il successivo relatore Armando Brath ha messo in evidenza la questione delle perdite di acqua che in Italia ammontano al 45% e in agricoltura sono ancora maggiori. Piero Sirini ha sollecitato la creazione di un sistema digitale che possa prendere decisioni autonome e semplificare (per esempio controllo da remoto, controllo dei parametri di processo). Sull'importanza dei dati e realizzazione di modelli predittivi si è soffermato anche Maurizio Porfiri a proposito delle alluvioni negli USA e della raccolta, analisi e diagnosi dei dati nonché sviluppo di modelli predittivi e della conseguente possibile attività informativa e di supporto alla PA. Sempre in relazione all'acqua, questa volta del mare, Fabio Filianoti e John Albertson hanno illustrato la loro ricerca sull'energia rinnovabile sfruttando il moto ondoso e le correnti marine sottolineando il supporto determinante del Machine Learning e la possibilità di comprendere meglio con l'ausilio dell'IA le soluzioni.

A conclusione della tavola rotonda è stata letta la mozione finale dove si precisa che «circa tremila Ricercatori, molti dei quali Universitari, opportunamente organizzati, si propongono di collaborare con il Governo assicurando una continua consulenza scientifica transdisciplinare sia per la previsione e prevenzione, manutenzione inclusa, sia per l'emergenza e il ritorno alla normalità a seguito di eventi idrogeologici ed idraulici significativi».

Talk to the Future Week, Milano, 10-14 luglio 2023

Organizzata dall'Ordine degli Avvocati di Milano la manifestazione ha riguardato i temi della transizione digitale e dell'IA. In tale occasione il Presidente del Consiglio Nazionale Forense, Avv. Francesco Greco, ha annunciato la realizzazione di «un portale dell'avvocatura italiana, basato sull'intelligenza artificiale, da mettere gratuitamente a disposizione di tutti, degli avvocati, ma anche dei cittadini e dei magistrati. E sarà un portale certificato, con la certezza che i dati che vengono immessi siano completi e

verificati. Ovviamente il portale costituirà una indicazione, ma poi servirà l'affinamento giuridico degli avvocati, a cui spetta l'ultima parola».

Gli scenari gestionali e assicurativi nella sanità italiana – Il contributo dell'intelligenza artificiale, Roma, 8-9 giugno 2023

Patrocinato anche dall'ANIA e Sapienza Università di Roma il convegno conferma la crescente centralità dell'IA anche in ambito sanitario e assicurativo. Tra gli argomenti delle numerose relazioni che si sono succedute su questi temi vanno ricordati quelli sulla gestione dei sinistri (U. Guidoni), riguardanti la medicina legale (L. La Russa e M. Cingolani), sull'IA in ambito INAIL (R. Rossi) e INPS (R. Migliorini), sulla valutazione globale della persona (D. Rodriguez).

Intelligenza artificiale, diritti, giustizia e pubblica amministrazione, Roma, Palazzo Spada, 18 maggio 2023

Nel corso del Convegno organizzato dall'Ufficio studi e formazione della Giustizia Amministrativa, suddiviso in due sezioni, la prima dal titolo "L'intelligenza artificiale e l'impatto sull'ordinamento costituzionale", la seconda "Intelligenza artificiale, giustizia e amministrazione", sono state tra l'altro trattate le questioni della tutela dei dati, delle procedure automatizzate, dei sistemi di elaborazione del linguaggio naturale, della giustizia predittiva e dei servizi digitali di interesse generale.

Riferimenti bibliografici

G. Buttazzo (2002), *Coscienza artificiale: missione impossibile*, in "Il mondo digitale", marzo 2002, n. 1

L. Califano (2023), *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati*, in "federalismi.it", 2023, n. 10

C. Caporale, L. Palazzani (a cura di) (2023), *Intelligenza Artificiale: distingue frequenter. Uno sguardo interdisciplinare*, Cnr Edizioni, 2023

L. Floridi (2023), *AI as* Agency Without Intelligence*: on ChatGPT, Large Language Models, and Other Generative Models*, in "Philosophy & Technology", March 2023

S. Hameroff, R. Penrose (2014), *Consciousness in the universe: a review of the 'Orch OR' theory*, in "Physics of Life Reviews", vol. 11, 2014, n. 1

N.A. Kissinger, E. Schmidt, D. Huttenlocher (2023), *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, Mondadori, 2023

N. Lucchi (2023), *ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems*, in "European Journal of Risk Regulation", June 12, 2023

S.M. Mayinger (2017), *Die künstliche Person*, Recht und Wirtschaft GmbH, 2017

J. Mc Fadden (2020), *Integrating information in the brain's EM field: the cemi field theory of consciousness*, in "Neuroscience of Consciousness", vol. 2020, n. 1, 2020

F. Pizzetti (2023), *Con AI Verso la Società digitale*, in "federalismi.it", 2023, n. 23

G. Taddei Elmi (2017), *Introduzione alle lezioni su* Roboetica. Dall'algoritmo all'umanoide, in *Atti e memorie dell'Accademia toscana di scienze e lettere La Colombaria*, vol. LXXXII, n.s. LXVIII, Leo S. Olschki, 2017

G. Taddei Elmi (1990), *I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum?*, in L. Lombardi Vallauri (a cura di), "Il meritevole di tutela", Giuffrè, 1990

S. Viggiani (2023), *Data mining Savio utilizzato dall'INPS: è stato trattamento illegittimo?*, in "Il Quotidiano Giuridico", 23 marzo 2023

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0128 • articolo non sottoposto a peer review • pubblicato in anteprima il 24 gen. 2024

OSSERVATORIO SU

Intelligenza Artificiale e diritto

coordinato da Giancarlo Taddei Elmi

GIANCARLO TADDEI ELMI - SOFIA MARCHIAFAVA

Sviluppi recenti in tema di Intelligenza Artificiale e diritto

Una rassegna di legislazione, giurisprudenza e dottrina

novembre-dicembre 2023

G. Taddei Elmi è ricercatore associato presso l'IGSG/CNR di Firenze. S. Marchiafava è avvocato cassazionista, LLM in Comparative Law, docente del Master di II livello in Informatica giuridica, nuove tecnologie e diritto dell'informatica presso Sapienza - Università di Roma

A. Normativa

1. Iter legislativo della proposta di legge sull'intelligenza artificiale - procedimento 2021/0106/COD

Il 9 dicembre 2023, dopo tre giorni di intensi negoziati, è stato raggiunto tra il Consiglio e il Parlamento europeo l'atteso accordo provvisorio sulla proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (*legge sull'intelligenza artificiale*) e modifica alcuni atti legislativi dell'Unione, presentata dalla Commissione europea il 21 aprile 2021, COM(2021) 206.

I negoziati e il raggiungimento dell'accordo in questione sono stati preceduti dall'orientamento generale adottato dal Consiglio il 6 dicembre 2022 e dall'approvazione della posizione negoziale del Parlamento europeo votata nella seduta plenaria del 14 giugno 2023 insieme agli emendamenti introdotti al testo della proposta, P9_TA(2023)0236.

Come sottolineato dalla Presidente della Commissione europea, Ursula von der Leyen, la cosiddetta Legge sull'IA o *AI Act* è una tappa fondamentale per l'Unione europea e un primo rilevante punto di riferimento normativo a livello globale.

Durante la conferenza stampa tenutasi subito dopo l'approvazione dell'accordo provvisorio, Carme Artigas, Segretario di Stato spagnolo per la digitalizzazione e l'IA, e Thierry Breton, Commissario europeo per il mercato interno, hanno evidenziato che si tratta a livello europeo di un risultato storico, una significativa "pietra miliare verso il futuro" che consente di affrontare la questione della rapida evoluzione tecnologica bilanciando l'esigenza di promuovere l'innovazione e l'adozione dell'IA nell'Unione europea, nel pieno rispetto dei diritti fondamentali dei cittadini, fornendo certezza al mercato. I correlatori del Parlamento europeo Brando Benifei (Commissione per il mercato interno e la protezione dei consumatori) e Dragoş Tudorache (Commissione per le libertà civili, la giustizia e gli affari interni) hanno illustrato alcuni dei punti principali esprimendo soddisfazione per la regolamentazione attenta ai valori europei e fondata su un approccio antropocentrico.

Il testo di compromesso sarà sottoposto nelle prossime settimane all'approvazione formale dello stesso Consiglio e Parlamento europeo, come annunciato nel comunicato stampa del 9 dicembre 2023.

Aspettando la pubblicazione del testo definitivo, che consentirà di stabilire l'effettivo contenuto della regolamentazione approvata rispetto alla proposta iniziale della Commissione europea, le principali novità dell'accordo provvisorio dovrebbero riguardare:

- i sistemi generali di IA ovvero utilizzabili per diversi scopi;
- il rafforzamento della governance;
- la possibilità di utilizzare l'identificazione biometrica remota da parte delle autorità di contrasto negli spazi pubblici solo entro limiti precisi e in alcune specifiche circostanze (terrorismo, ricerca di persone scomparse, gravi crimini);
- i requisiti di trasparenza richiesti ai sistemi di IA generativa;
- la valutazione di impatto dei sistemi di IA sui diritti fondamentali, preliminare all'immissione dei sistemi di IA nel mercato.

Si tratta di una normativa auspicata da molti, a livello nazionale, per esempio, dal Garante per la protezione dei dati personali che nelle scorse settimane aveva paventato il mancato raggiungimento dell'accordo.

Un *AI Pact* dovrebbe impegnare su base volontaria gli sviluppatori di IA europei e del resto del mondo ad attuare gli obblighi previsti dalla Legge sull'IA o *AI Act* nel periodo precedente alla sua effettiva entrata in vigore.

Sofia Marchiavava

B. Dottrina

1. Glosse sulla "soggettività" della Intelligenza Artificiale

1.1 Immaginazione ed emozione, ultime soglie dell'"umano" anche nell'era della Intelligenza artificiale "generativa"?

Il libro di Yuval Noah Harari, *Sapiens. Da animali a Dèi. Breve storia dell'umanità*, edito da Bompiani nel 2014 e riproposto nel dicembre 2023 da Il Sole 24, ci riporta al grande cruciale problema della differenza ultima tra macchina e uomo.

Nella prima di copertina si legge che «il segreto del nostro successo [n.d.r. dell'Homo Sapiens] è l'immaginazione. Siamo gli unici animali capaci di parlare di cose che esistono solo nelle nostre fantasie: come le divinità, le nazioni, le leggi e i soldi».

Nel 2002, in *Riduzionismo e oltre*, Luigi Lombardi Vallauri indicava i livelli a cui può essere accertata l'immaterialità della mente, e oltre alla sensazione "sentita", l'intellezione semantica del discorso *totum simul*, la consapevolezza di sé, la vera autonomia di scelta, attribuiva un ruolo direi determinante alla immaginazione o fantasia. «Caratteristica della immaginazione o fantasia, rispetto alla sensazione o percezione, è che con l'immaginazione io mi rappresento degli enti sensibili, materiali anche in loro assenza, ossia senza che vengano esercitate sui miei organi percettivi azioni fisiche misurabili provenienti dal mondo circostante. Io posso "vedere" a occhi chiusi o al buio, "udire" nel silenzio. Mentre la sensazione ha una sua ubicazione precisa, l'immaginazione è per così dire "extraterritoriale" Al tempo stesso l'immaginazione è solo di oggetti materiali, accessibili a uno almeno dei sensi esterni: possiamo avere solo immagini visive, acustiche, tattili, olfattive, gustative o loro combinazioni. Abbiamo immagini di oggetti fisici, non connotati della singolarità. Non abbiamo immagini (di) universali» (Lombardi Vallauri 2002, p. 39).

Credo che questa dote, non ancora raggiunta dai recenti vertiginosi sviluppi della Intelligenza artificiale cd. generativa, resterà a lungo il limite invalicabile anche da parte di future 'intelligenze', che si preconizza potrebbero superare quelle degli umani. Ma si tratterà sempre di intelligenze *super* ma morfo-sintattiche, non semantiche, inconsapevoli delle proprie azioni e delle cd. auto-determinazioni algoritmico-neurali.

Una recentissima intervista televisiva a Mauro Lombardi, economista fiorentino, autore nel 2017 di *L'esplosione robotica e il futuro incerto dell'umanità, Roboetica. Per un ciclo di Lezioni Dall'algoritmo all'umanoide* (edito in Atti e memorie dell'Accademia Toscana di Scienze e Lettere La Colombaria, vol. LXXXII, Nuova serie, 2017, Leo S. Olschki Editore, pp. 381-391), aggiunge un ulteriore elemento di riflessione importante alla discussione uomo-macchina e cervello-mente.

Asserisce Lombardi che le macchine conoscono e apprendono in modo razionale e non emotivo. Nel cervello umano si addenserebbero conoscenze acquisite attraverso meccanismi logici ed esperienze che producono emozioni. Questo patrimonio emozionale sarebbe l'elemento che concorrerebbe con la ragione a "generare" (meglio in questo caso a "creare") azioni e decisioni autenticamente "nuove".

Oltre all'aspetto "emozionale", Mauro Lombardi sottolinea l'aspetto meramente "statistico-probabilistico" della Intelligenza Artificiale "generativa", che ri-produce azioni e decisioni implicite già esistenti. La macchina non produce nulla di veramente nuovo, ma assemblaggi "diversi" di dati pre-esistenti nella Rete non inclusivi delle esperienze emotive dei "singoli".

Concordo pienamente sia sulla non "emozionalità" della IA sia sulla sua intrinseca "aritmeticità-matematicità" non qualitativa. La IA rappresenta in maniera "innovativa" cose già espresse ed elaborate in contesti diversi. Sono sintesi statistiche di elementi precedenti presentati in modo nuovo, non creazioni veramente "nuove". Sono dei "nova" apparenti, perché, anche se raggiunti con una autonomia, si fondano su trattamento di conoscenze solo "razionali" già note. Sono dei prodotti generati dalla Rete, sulla base di dati tutti interni alla Rete, senza alcun apporto esterno se non il programma di lancio iniziale. Dunque non "creati" come i prodotti umani che sono il risultato sia di una *pregressa esperienza consolidata sia di una immediata e contingente valutazione emotiva e assiologica.* L'originalità degli esiti di IA consiste nella espressione formale non nella sostanza.

Questa riflessione trova pieno conforto in ciò che recentemente ha scritto Luciano Floridi, definendo i sistemi di IA generativi dei "pappagalli stocastici" produttori di sintesi "non nuove" ma solo aggregate in modo "nuovo"[1].

In realtà Floridi è ancora più drastico: non solo sottolinea la "non novità" del prodotto dei modelli linguistici (LLMs), che si limiterebbero solo a «synthesises texts (n.d.r.: già noti) in new way», ma anche ribadisce che tali sistemi stocastici ripeterebbero testi senza comprendere nulla e per questo privi di *Intelligence* (vedi titolo del saggio).

Su questo mi sentirei di alleggerire la posizione, negando ai sistemi di IA non l'intera "intelligenza" ma solo quella parte di "intelligenza" che chiamiamo comprensione del significato. Sono strumenti che riconoscono perfettamente la morfologia e la sintassi del linguaggio ma non la semantica. Per dirla con De Saussure, riconoscono i *signifiants* del "discorso" e la loro sequenza ma non ne capiscono i *signifiés*.

Quanto alla non emozionalità della IA, un esempio calzante può essere tratto dagli esperimenti di "arte artificiale": il celebre progetto *Next-Rembrandt*, che aspirerebbe a produrre "nuovi Rembrandt", in realtà ri-produce un dipinto che è una combinazione tecnologica di molti "Rembrandt" (esempio ritratti) già prodotti.

Un "Rembrandt" reincarnato, che volesse rappresentare una copia esatta della "Ronda di Notte", sfrutterebbe, indubbiamente, il disegno e la tecnica dell'originale esposto al museo di Amsterdam, ma vi trasfonderebbe certamente anche un afflato di stati d'animo contingenti. Il colore delle spade o dei cappelli, influenzato dalle emozioni che in quegli istanti pervadono l'artista, forse sarebbe diverso. Questo sarebbe un vero Next-Rembrandt.

Tre sono in definitiva i limiti insuperabili dalla IA anche generativa, la comprensione del "significato", l'astrazione dei "concetti" e l'esperienza delle "emozioni". Ricordo che ci stiamo muovendo sempre sul piano delle macchine inconsapevoli dunque non "soggettive". Limiti sempre "meccanici" o "robotici", "oggettivi".

Se vogliamo davvero varcare la soglia che separa l'oggettività dalla soggettività dobbiamo incamminarci in un percorso complicato che costringe a indagare sulla capacità delle macchine di pensare se stesse. Ma come facciamo a capire se pensano un sé non essendo dentro quelle macchine o essendo proprio quelle macchine. Alan Turing taccia l'argomento della coscienza di sé come solipsistico e considera forse valido solo quello della capacità "extrasensoriale" (A. Turing, *Calcolatori e intelligenza,* in D.R. Hostadter e D.C. Dennett (a cura di), "L'Io della mente", Adelphi, Milano, 1985, pp. 63-74).

Ma su queste ultime suggestioni ci soffermeremo in una prossima nota. Per ora occupiamoci della IA generativa che mostra già forti limiti oggettivi. Ripartiremo dalla obbiezione di Sir Geoffrey Jefferson, illustrata nella *Lister Medal Oration* al *Royal College of Surgeons of England* del 1948 e pubblicata con il titolo *The Mind of Mechanical Man* (in "The British Medical Journal", vol. 1, Jun. 25, 1949, n. 4616, pp.

1. Floridi 2023, p. 3.

1105-1110), che nega alle macchine la capacità di scrivere sonetti e comporre concerti sulla base di pensieri propri ed emozioni provate e dunque la coscienza di sé e la soggettività.

Oggi però l'IA generativa compone sonetti e compone concerti ….?!

Giancarlo Taddei Elmi

1.2 Il dibattito tra gli psicologi sulla IA "cosciente"

Chiara Cilardo in *Le intelligenze artificiali possono avere una coscienza? - Psicologia digitale*, pubblicato il 6 ottobre 2023 e aggiornato il 17 ottobre 2023, sostiene che eseguire grandi elaborazioni di dati non significa esserne consapevoli: la coscienza tipicamente umana non sembra estendersi alle tecnologie.

Nel 1990 Giancarlo Taddei Elmi[2] si chiedeva se i sistemi informatici iper-intelligenti potessero superare la grande dicotomia cosa-persona assumendo una qualche forma di soggettività. Si distingueva tra soggettività ontologica e soggettività ascritticia in base al possesso o meno di requisiti essenziali quali la sensazione-percezione, la immaginazione-fantasia, la intellezione, la autocoscienza e la autodeterminazione. La risposta dell'epoca era necessariamente negativa essendo le macchine prive di sensazioni "sentite", di rappresentazione concettuali, di consapevolezza di sé e di scelte realmente autonome non etero-programmate.

Nel 2002 Giorgio Buttazzo[3] lanciava la provocatoria suggestione che i sistemi di IA avrebbero potuto nel 2029 assumere stati di coscienza sulla base di uno sviluppo delle loro capacità di calcolo: a quella data le RAM dei calcolatori avrebbero raggiunto la possibilità di elaborare connessioni 10 alla 15 pari a quelle del cervello biologico. Questa posizione dava per scontata le tesi monistica che la mente abbia sede tutta nel cervello e che gli stati soggettivi siano prodotti esclusivamente da scariche elettriche e non anche da processi biochimici e fisici come l'energia prodotta da vibrazioni quantiche dei microtuboli cerebrali (Teoria Orch-or di Hameroff e Penrose[4]) o da vibrazioni elettromagnetiche sempre prodotte dai neuroni[5].

Ma a parte questa obiezione scientifica, ve ne era una logica pregiudiziale ossia che il raggiungimento di quella elevata capacità di calcolo sarebbe in ogni caso una condizione necessaria ma non sufficiente per dimostrare che quelle macchine così dotate fossero coscienti.

Del resto anche i sistemi di IA ad apprendimento autonomo degli anni 2000, benché in qualche modo imprevedibili nei risultati, sono sempre guidati da algoritmi esecutivi di istruzioni fornite totalmente dal programmatore o almeno da algoritmi di obbiettivo. Il ruolo umano è ancora determinante.

Esigenze *de iure condendo*, in relazione agli esiti delle azioni dei sistemi di IA sempre più imprevedibili, costringono il giurista e il legislatore a immaginare soluzioni per colmare certi gap (lacune) normativi in materia di attribuzione di responsabilità: al costruttore, al programmatore o all'utilizzatore o a nessuno?

Si propongono principalmente le ipotesi di responsabilità oggettiva ben note ai sistemi giuridici, quali *culpa in eligendo*, *culpa in educando*, per attività pericolosa, per custodia di cose e animali, etc. Ma alcuni, e la stessa Unione europea attraverso il suo Parlamento, avanzano una ipotesi, inizialmente considerata a torto fanta-giuridica perché non compresa appieno, di riconoscere (meglio di attribuire) uno status giuridico di persona elettronica ai sistemi più sofisticati e più autonomi. Ovviamente si trattava di una soggettività ascritticia concretizzata nella figura della personalità giuridica ben nota a tutti gli ordinamenti giuridici. Queste entità giuridiche fittizie potrebbero essere dotate di patrimoni alla stregua del *peculium* dei servi romani o di altri tipi di fondi o anche di coperture assicurative.

2. Taddei Elmi 1990.
3. Buttazzo 2002.
4. Il modello ORCH-OR (*ORCHestrated Objective Reduction*) è un modello della mente ideato da Roger Penrose e Stuart Hameroff. L'idea centrale dell'ipotesi è che la coscienza nel cervello origini da un processo che avviene all'interno dei neuroni, piuttosto che nell'interazione tra di essi.
5. McFadden 2002.

Di fronte alla sfida tecnologica della IA generativa, che agisce autonomamente producendo risultati in modo empirico a posteriori sulla base di elaborazioni statistico probabilistiche di dati noti tratti dalla Rete, dobbiamo riproporci il dilemma cosa-persona? Questa IA così quantitativamente potente e imprevedibile, ultra-autonoma rispetto al programmatore, è "un po' cosciente" (*slightly conscious*) come nel 2022 ha scritto su Twitter Ilya Sutskever, uno dei fondatori e Chief Scientist di OpenAI, la società che ha sviluppato ChatGPT.

Chiara Cilardo in proposito sostiene che le intelligenze artificiali cd. generative non hanno coscienza perché il solo fatto di eseguire grandi elaborazioni di ampie masse di dati non significa esserne consapevoli: la IA agirebbe in uno status privo di esperienze proprie, di personalità, di motivazioni "volute" e di automonitoraggio. Secondo gli psicologi esisterebbero due dimensioni della coscienza: una introspettiva, in prima persona, di automonitoraggio in cui il soggetto è in grado di osservare i propri processi cognitivi come memoria, apprendimento, attenzione, elaborazione delle informazioni, insomma la metacognizione[6] (la coscienza fenomenica di Block?[7]) e una seconda chiamata "disponibilità globale" ossia l'insieme delle informazioni disponibili in un dato momento (la coscienza dell'"accesso" di Block?)[8]; le tecnologie lavorerebbero, in modo più o meno elaborato, su questa seconda dimensione. Per cui anche se vengono progettate analogamente alla mente umana in termini di specifiche funzioni e processi, sarebbero prive di metacognizione, incapaci di automonitoraggio e introspezione[9].

Anche di fronte al problema così posto ci sentiamo di escludere nettamente che la IA generativa attuale possieda la dimensione di coscienza introspettiva o fenomenica; si potrebbero forse aprire scenari nuovi verso la coscienza della disponibilità globale (dell'accesso).

Ma ritengo che un sistema con accesso globale a tutta la conoscenza possibile, elaborata in modo meramente statistico, non si renda conto delle sue azioni. Questo ovviamente lo presumiamo e non ne abbiamo la certezza; la avremmo solo se fossimo dentro quella macchina come sostiene Turing nel celebre *Computing Machinery and Intelligence* ("Mind" 1950, p. 236).

Gli scenari di una IA cosciente si potrebbero aprire quando il progresso tecnologico si incamminasse in due direzioni sia verso l'implementazione di computazioni che riflettono i processi dell'inconscio[10] sia verso la progettazione di interfacce cervello computer (*Brain Computer Interface*), destinate ad aumentare le capacità del cervello umano[11]. Le IA attuali tentano di simulare o sostituire una piccola parte dell'intelligenza umana. Una IA dell'Oltre dovrebbe mirare a produrre intelligenze dotate di immaginazione, emozioni, intuizioni, conoscenza implicita o tacita e anche intelligenze individuali[12].

Giancarlo Taddei Elmi

2. Saggi e volumi

A. Alaimo, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in "federalismi.it", 2023, n. 25, pp. 133-149

6. Dehaene-Lau-Koudier 2017, pp. 486-487. L'automonitoraggio corrisponde alla introspezione («a self-referential relationship in which the cognitive system is able to monitor its own processing and obtain information about itself»). La coscienza introspettiva è analoga alla coscienza fenomenica di Block 1995.
7. Block 1995.
8. Hildt 2019 (*Artificial Intelligence: Does Consciousness Matter? - PubMed (nih.gov)*). La *Global availability* richiamerebbe la *Access consciousness* di Block.
9. Cilardo 2023.
10. Dehaene-Lau-Kouider 2017.
11. Dong-Hou-Zhang-Zhang 2020.
12 Dong-Hou-Zhang-Zhang 2020 e Shruthi 2023.

Il contributo confronta il testo di Regolamento sull'Intelligenza Artificiale (*AI Act*) proposto dalla Commissione europea il 21 aprile 2021 e quello approvato dal Parlamento il 14 giugno 2023, evidenziando l'introduzione nel testo emendato di maggiori garanzie per i valori e i diritti fondamentali dell'Unione europea, gli obiettivi sociali e la tutela dei lavoratori.

U. Bechini, L*'intelligenza artificiale, i notai e l'avvocato Schwartz*, in "Notariato", 2023, n. 6, pp. 605-610

L'Autore si interroga sull'effettivo impatto dell'IA sulla professione notarile, sui suoi limiti e i suoi rischi, rilevando come sia il contesto giuridico e il modello organizzativo della stessa professione a determinare il successo degli strumenti di IA, le difficoltà di raccolta dei dati necessari all'addestramento e per riversare nel software il know-how acquisito dai professionisti, L'Autore si sofferma anche sulle conseguenze degli ingenti investimenti tecnologici.

A. Prencipe – M. Sideri, *Il visconte cibernetico. Italo Calvino e il sogno dell'intelligenza artificiale*, Luiss University Press, 2023

Con la prefazione di Maria Chiara Carrozza, Presidente del CNR, il saggio è stato presentato il 6 dicembre 2023 in occasione di una tavola rotonda organizzata a Roma presso l'Università Luiss Guido Carli. Tra le numerose riflessioni e richiami a illustri pensatori e scienziati il saggio evidenzia lo stretto rapporto tra intelligenza umana e IA, la capacità di interrogarsi propria dell'uomo e quella di fornire risposte oggi anche dei sistemi di IA. Una recensione del volume a firma di Maurizio Ferraris e dal titolo *Artificiale. Umanissima*, apparsa il 3 gennaio 2024 sul Corriere della Sera, paventa il rischio concreto di «un uso malevolo di questa nuova forza» piuttosto che il sopravvento dell'IA sull'umanità.

C. Giurisprudenza

– Opere dell'ingegno e IA negli USA

Un interessante caso a proposito delle implicazioni e questioni giuridiche, sollevate riguardo alle opere (letterarie, musicali, artistiche, ecc) create utilizzando sistemi di IA e l'impiego di materiali protetti da copyright nell'addestramento di tali sistemi per generare nuovi contenuti dovrà essere deciso nei prossimi mesi negli Stati Uniti d'America a seguito del giudizio instaurato il 27 dicembre 2023 dalla società "The New York Times Company" (d'ora innanzi "NY Times"), davanti alla Corte distrettuale degli Stati Uniti d'America - Distretto meridionale di New York, contro le società Microsoft Corporation ("Microsoft") e OpenAI, Inc., OpenAI LP, OpenAI GP LLC, OpenAI LLC, OpenAI OpCo LLC, OpenAI Global LLC, OAI Corporation, LLC, OpenAI Holdings, LLC (d'ora in poi Microsoft e OpenAI) per contestare la violazione dei suoi diritti di copyright (*17 U.S.C. § 501 - Copyright Infringement*), gli atti di concorrenza sleale (*Common Law Unfair Competition By Misappropriation*), e, infine, la diluizione della forza del suo marchio (*Trademark Dilution (15 U.S.C. § 1125(c)*).

In particolare, come si legge nel suo lungo atto introduttivo (*complaint*), la società NY Times, che vanta attraverso il suo prestigioso quotidiano dieci milioni di abbonati, ha esercitato in sede giudiziale un'azione risarcitoria e inibitoria, contestando l'utilizzo non autorizzato e la riproduzione dei suoi contenuti da parte delle società convenute Microsoft e OpenAI ai fini dell'IA generativa ovvero per addestrare i prodotti GPT, GPT-2, GPT-3, GPT-3.5 e GPT-4 fondati sul *large language model* (LLM). Ad esempio, per GPT-2 il dominio *NYTimes.com* risulta uno dei "primi 15 domini per volume" ed è elencato come il quinto "dominio principale" nel set di dati utilizzati per tale addestramento.

A dimostrazione della fondatezza delle sue pretese la società NY Times riporta alcuni esempi concreti e richiama alcune dichiarazioni e condotte di natura confessoria delle società convenute.

In aggiunta alla contestazione dell'incorporazione di riproduzioni non autorizzate nei Modelli GPT, alla visualizzazione pubblica non autorizzata di sue opere negli output dei prodotti GPT, alla conservazione e diffusione non autorizzata di notizie attuali, la società NY Times deduce l'intenzionalità delle rispettive violazioni chiedendo in conclusione, insieme al risarcimento dei danni, la cessazione della

condotta contestata, la distruzione dei GPT o di altri LLM e set di addestramento che incorporano i suoi prodotti, oltre al rimborso dei costi e delle spese legali nonché qualsiasi altro ulteriore provvedimento ritenuto dalla Corte adeguato anche in via equitativa.

Riguardo alla pretesa risarcitoria la Corte statunitense dovrà anche pronunciarsi sulle cosiddette "allucinazioni", contenuti attribuiti erroneamente al quotidiano che oltre a causare un danno commerciale alla società NY Times determinano disinformazione e, quindi, un danno alla collettività.

Sofia Marchiafava

D. Attività internazionali

1. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (E.O. 14110, USA)

Il 30 ottobre 2023 il Presidente degli Stati Uniti d'America, Joseph R. Biden, ha firmato l'*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, un provvedimento che indirizza l'azione e le politiche a livello federale sull'IA.

Composto da 13 Sezioni, questo manifesto americano sull'IA esordisce alla Sezione 1 (*Purpose*) sottolineandone lo straordinario potenziale, sia verso aspettative (*Promise*) sia verso rischi (*Peril*), che richiede per il bene di tutti una alta responsabilità del governo, del settore privato, dell'accademia e della società civile.

Nella Sezione 2 (*Policy and Principles*) si evidenziano otto principi guida e priorità che l'Amministrazione del Presidente Biden intende seguire in relazione allo sviluppo della IA: sicurezza; innovazione, concorrenza responsabile e collaborazione con investimenti anche in formazione; sostegno dei lavoratori; equità e diritti civili, protezione dei consumatori, tutela delle libertà civili e della riservatezza, controllo, gestione dei rischi e regolamentazione da parte del governo federale.

La Sezione 3 (*Definitions*) è un ampio e utile dizionario dei termini usati nel provvedimento presidenziale (*agency, artificial intelligence, machine learning*, ecc.).

Nella Sezione 4 (*Safety and Security*) vengono assegnati precisi compiti, impegnando diffusamente 30 agenzie pubbliche a livello federale, per individuare entro determinate scadenze (l'ultima gennaio 2025), linee guida, standard, buone pratiche e regole al fine di garantire la sicurezza e l'affidabilità in relazione all'IA anche con riferimento alle infrastrutture critiche, alla cybersecurity e per la riduzione dei rischi connessi.

La Sezione 5 illustra i modi per promuovere innovazione e concorrenza, quali l'attrazione di talenti stranieri competenti in IA facilitandone la permanenza negli USA, la creazione di partenariati pubblico-privati, il sostegno al settore dei semiconduttori.

Nella Sezione 6 si ribadisce l'esigenza di garantire e sostenere il lavoro indicando le specifiche azioni da intraprendere in tale direzione, per esempio attraverso studi, programmi di sostegno e formazione.

La Sezione 7 è dedicata alla promozione dell'equità e dei diritti civili, con il rafforzamento dell'IA in ambito penale, la tutela contro possibili discriminazioni riguardo ai benefici e programmi governativi nonché nelle assunzioni e in relazione alle disabilità.

La Sezione 8 indica le azioni per tutelare i consumatori, pazienti, passeggeri e studenti, sollecitando le agenzie di regolamentazione indipendenti a prendere in considerazione l'esercizio dei rispettivi poteri contro frodi, discriminazioni, minacce alla privacy e altri rischi derivanti dall'uso dell'IA, in particolare attraverso la regolamentazione, l'indicazione delle normative e linee guida esistenti e applicabili, nonché mediante la l'individuazione delle responsabilità.

La Sezione 9 sulla protezione della privacy assegna specifici compiti a diversi organismi federali (*Office of Management and Budget, Federal Privacy Council, Interagency Council on Statistical Policy*, ecc.),

anche attraverso la ricerca, lo sviluppo e l'implementazione delle tecnologie di miglioramento della privacy (PETs).

La Sezione 10 illustra i modi e le linee guida per l'avanzamento dell'uso della IA da parte del Governo federale, mediante linee guida sulla gestione della IA, la pianificazione delle iniziative a livello globale, ad esempio per promuovere e sviluppare standard condivisi.

La Sezione 11 si riferisce all'intento di rafforzare la leadership statunitense in ambito globale, con iniziative da intraprendere da parte del Segretario di Stato e dei collaboratori del Presidente per gli affari di sicurezza nazionale e per la politica economica, del Direttore dell'Ufficio per le politiche scientifiche e tecnologiche nonché dei vertici di altre agenzie competenti.

La Sezione 12 (*Implementation*) prevede l'istituzione del Consiglio per l'IA della Casa Bianca (*White House AI Council*), con funzione di coordinamento delle attività delle agenzie federali per garantire l'efficace formulazione, sviluppo, comunicazione, e attuazione tempestiva delle politiche relative all'IA.

La Sezione 13 (*General Provisions*) stabilisce in conclusione alcune disposizioni generali per chiarire il rapporto con la normativa vigente precisando che, oltre a essere a quest'ultima conforme, l'*Executive Order* non attribuisce alcun diritto o beneficio a carico degli Stati Uniti d'America, dei suoi dipartimenti, delle sue agenzie o entità, dei suoi funzionari, dipendenti, agenti o di altri soggetti.

Sofia Marchiafava

2. The Bletchley Declaration

Un'altra iniziativa a livello internazionale, che si segnala per la sua rilevanza, è la dichiarazione sottoscritta (da 29 paesi tra cui USA, UK, Giappone, Italia) in occasione dell'*AI Safety Summit 2023* tenutosi il 1 e 2 novembre 2023 in UK, Bletchley Park, Buckinghamshire, che sancisce a livello globale l'esigenza di progettare, sviluppare, implementare e utilizzare l'IA in modo sicuro, affidabile e responsabile assicurando la centralità dell'uomo.

Nel sottolineare l'importanza di misurare, monitorare e mitigare le capacità potenzialmente dannose dei sistemi di IA, anche per prevenire abusi e problemi di controllo e l'amplificazione di altri rischi, nella dichiarazione si afferma che nel contesto della cooperazione internazionale l'agenda è volta a identificare i rischi per la sicurezza e a stabilire una comprensione scientifica condivisa.

3. Hiroshima Process International Guiding Principles and Code of Conduct for Organizations Developing Advanced AI system

L'Unione europea coopera a livello internazionale nell'ambito del G7 e G20 nonché con importanti organizzazioni (OCSE, Nazioni Unite, ecc.) al fine di promuovere regole e standard comuni e globali.

In tale contesto l'Unione europea ha sostenuto l'accordo raggiunto il 30 ottobre 2023 dai leader del G7 riuniti a Hiroshima, Giappone, sui principi guida internazionali *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system* e il codice di condotta volontario per gli sviluppatori di sistemi di IA avanzati *Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems* per coloro che sviluppano sistemi di IA avanzati, compresi i modelli di base e i sistemi di IA generativa più avanzati.

Nell'ambito degli undici principi individuati per coprire la progettazione, lo sviluppo, l'implementazione e l'uso di sistemi avanzati di IA, è prevista: l'adozione di misure adeguate per identificare, valutare e mitigare i rischi durante il ciclo di vita dell'IA; la precedenza alla ricerca per mitigare i rischi sociali e per la sicurezza nonché per definire le priorità degli investimenti in misure di mitigazione efficaci; la promozione dello sviluppo e, se del caso, l'adozione di norme tecniche internazionali.

E. Eventi, seminari, convegni, notizie

– Cybersecurity e IA: sfide e tutele per i cittadini europei

Il 18 dicembre 2023, presso il Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche, dell'Università degli Studi Roma Tre, si è tenuto un Convegno dedicato alle nuove regolamentazioni dell'Unione europea sulla Cybersecurity e IA e relative interazioni.

– Gli Stati Generali del Diritto di Internet e dell'IA

La terza edizione del convegno, a cura di Francesco Di Ciommo e Giuseppe Cassano, si è svolta dal 14 al 16 dicembre 2023, presso la Luiss, Roma, con autorevoli interventi sui temi del Diritto di Internet e dell'IA in relazione al Diritto civile, ai minori e al Diritto penale, al Diritto d'autore, Diritto commerciale, alla Privacy e Responsabilità sanitaria.

– Le intelligenze artificiali secondo il diritto. Riflessioni su modello regolatorio e governance del digitale

Seminario telematico del 7 dicembre 2023, con relatrice Marina Pietrangelo, IGSG/CNR, organizzato dall'Università degli Studi dell'Insubria, Dipartimento di Economia e Centro di ricerca sulla regolamentazione dell'Intelligenza Artificiale (CRIA).

– Intelligenza artificiale: pace o guerra?

Tavola rotonda, organizzata il 6 dicembre 2023 presso la Sapienza Università di Roma Dipartimento di Scienze sociali ed economiche, a partire dal volume "Dai droni alle armi autonome. Lasciare l'Apocalisse alle macchine?", Franco Angeli, 2023, a cura di Francesca Farruggia, con la prefazione di Giorgio Parisi e scritti di Fabrizio Battistelli, Sofia Bertieri, Francesca Farruggia, Barbara Gallo, Adriano Iaria, Diego Latella, Michael Malinconi, Giorgio Parisi, Juan Carlos Rossi, Maurizio Simoncelli, Gian Piero Siroli, Guglielmo Tamburrini.

Riferimenti bibliografici

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

U. Bechini (2023), *L'intelligenza artificiale, i notai e l'avvocato Schwartz*, in "Notariato", 2023, n. 6

N. Block (1995), *On a confusion about the function of consciousness, behavioral and brain*, in "Sciences", vol. 18, 1995, n. 2

G. Buttazzo (2002), *La coscienza artificiale: missione impossibile*, in "Il Mondo digitale", marzo 2002

C. Cilardo (2023), *Le intelligenze artificiali possono avere una coscienza?*, in "stateofmind.it", 2023

S. Dehaene, H. Lau, S. Kouider (2017), *What is consciousness, and could machines have it?*, in "Science", vol. 358, 2017, n. 6362

Y. Dong, J. Hou, N. Zhang, M. Zhang (2020), *Research on how human intelligence, consciousness, and cognitive computing affect the development of artificial intelligence*, in "Complexity", 2020

L. Floridi (2023), *AI as Agency Without Intelligence: on ChatGPT, Large Language Models, and Other Generative Models*, in "Philosophy & Technology", vol. 36, 2023

E. Hildt (2019), *Artificial intelligence: Does consciousness matter?,* in "Frontiers in Psychology", vol. 10, 2019, n. 1535

L. Lombardi Vallauri (2002), *Riduzionismo e oltre*, Cedam, 2002

J. Mc Fadden (2002), *Synchronous firing and its influence on the brain's electromagnetic field: Evidence for an electromagnetic field theory of consciousness*, in "Journal of Consciousness Studies", vol. 9, 2002, n. 4

A. Prencipe, M. Sideri (2023), *Il visconte cibernetico. Italo Calvino e il sogno dell'intelligenza artificiale*, Luiss University Press, 2023

R. Shruthi (2023), *Human consciousness and artificial intelligence: Can AI develop human-like consciousness? Cognitive abilities? What about Ethics?*, January 18, 2023

G. Taddei Elmi (1990), *I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum?*, in L. Lombardi Vallauri, E. Castrucci, M. Roncoroni et al. (a cura di), "Il Meritevole di tutela (Studi per una ricerca coordinata da Luigi Lombardi Vallauri)", Giuffrè, 1990

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0112 • articolo non sottoposto a peer review • pubblicato in anteprima il 21 set. 2023

Enrico Albanesi

Autorecensione a: Enrico Albanesi, Alessandra Valastro, Roberto Zaccaria, *Diritto dell'informazione e della comunicazione,* XII edizione, Milano, Wolters Kluwer-Cedam, 2023

La recensione ricostruisce, sinteticamente ma con dovizia di argomentazioni, il filo rosso della dodicesima edizione del Manuale E. Albanesi, A. Valastro, R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Milano, Cedam-Wolters Kluwer, 2023. Il Manuale analizza criticamente il principio costituzionale del pluralismo dei mezzi di informazione, che in Italia è stato elaborato dalla Corte costituzionale con riferimento alla radiotelevisione a partire dagli anni Settanta/Ottanta. Un principio ancora oggi presente nella giurisprudenza della Corte costituzionale e delle Corti europee, se pur da declinarsi con riferimento alle novità dell'ambiente tecnologico affermatosi, specie a partire dalla seconda metà degli anni Duemila, con la rivoluzione digitale e l'avvento del web 2.0. In tale innovativo contesto, l'esatta declinazione di tale principio rappresenta però per il costituzionalismo una sfida, a causa dell'ingresso di piattaforme online globali nella sfera pubblica. Il ruolo di tali piattaforme rischia di formare pericolosi nuovi "colli di bottiglia" nel sistema integrato delle comunicazioni e nel mercato unico digitale ed è quindi indispensabile in prima battuta riflettere sulla natura giuridica di tali piattaforme.

The review focuses on the common thread running through the twelfth edition of the handbook E. Albanesi, A. Valastro, R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Milano, Cedam-Wolters Kluwer, 2023, 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. However, such a principle should now be established with regard to the digital environment born with the digital revolution, the transformation of the Internet and the web 2.0 in the second half of the 2000s. The handbook argues that the implementation of the principle is a challenge for constitutionalism, due to the role played in the public sphere by online global platforms.

L'Autore è professore associato di Diritto costituzionale presso il Dipartimento di giurisprudenza dell'Università di Genova

1. Il Manuale *Diritto dell'informazione e della comunicazione* nacque nel 1996 sulla base dell'esperienza universitaria fiorentina e si è arricchito negli anni anche dell'esperienza pratica. È giunto quest'anno (2023) alla dodicesima edizione, che qui si recensisce.

L'analisi critica dello stato dell'arte del principio del pluralismo dei mezzi di informazione ha sempre costituito il filo rosso di ogni edizione del Manuale.

2. Tale principio fu elaborato nel nostro Paese dalla Corte costituzionale a partire dagli anni Settanta/Ottanta, con riguardo al settore radiotelevisivo. In tale settore, infatti, alla luce della scarsità delle frequenze nell'etere come mezzo trasmissivo, occorreva garantire la possibilità d'ingresso nel mercato radiotelevisivo del maggior numero possibile di soggetti, per quanto lo consentissero i mezzi tecnici (pluralismo esterno). Non solo. Appariva altresì indispensabile che la concessionaria pubblica diffondesse una gamma quanto più possibile vasta di opinioni, tendenze, correnti di pensiero politiche, sociali e culturali presenti nella società (pluralismo interno).

Ventisette anni dopo l'uscita della prima edizione, quello che ci si chiede in particolare in questa edizione è se l'esigenza costituzionale di garantire il principio pluralistico sia ancora attuale.

Sembrerebbe di no, ad un esame superficiale: la rivoluzione digitale, il processo di convergenza multimediale e lo sviluppo della rete Internet e del web 2.0 hanno infatti incrementato le potenzialità di accesso per nuovi soggetti al sistema dell'informazione e delle comunicazioni. 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. Non solo. La Corte di Cassazione ha ormai riconosciuto al "giornalismo diffuso" sulla rete Internet un ruolo essenziale nella società democratica ed una tutela pari a quello professionale, quantomeno nella prospettiva dei principi costituzionali[1].

La risposta che però emerge da questa edizione del Manuale è che il principio pluralistico sia ancora un'esigenza costituzionale meritevole di tutela nell'ambiente digitale che caratterizza l'attuale sistema dell'informazione e della comunicazione: non a caso, continuano a fare ad esso riferimento la Corte costituzionale[2] e le Corti europee[3].

Ancora nel 2022, il *Report* del *Centre for Media Pluralism and Media Freedom* dello *European University Institute* di Fiesole[4] segnalava l'elevato tasso di concentrazione del sistema di informazione del nostro Paese: elemento, quest'ultimo, che costituisce un fattore di rischio per il pluralismo dei media. Per tacere della perdurante assenza di una normativa in materia di conflitto d'interessi, problema segnalato dalla Commissione europea nel suo *Rapporto sullo Stato di diritto* in Italia ancora nel 2022[5]. In questo quadro, non ha certo aiutato l'inazione dell'Agcom, l'Autorità chiamata a vigilare in materia: tanto da trovare conferma le perplessità che si manifestavano nella scorsa edizione del Manuale sul fatto che (peraltro, come al solito

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* e Corte costituzionale, ordinanza 26 giugno 2020, n. 132, punto 7.1 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 e 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.
4. Cfr. Carlini-Trevisan-Brogi 2022, p. 14 s.
5. Cfr. Commissione europea 2022, p. 16.

in questo settore, con una normativa-ponte della durata di sei mesi) la "risposta" da parte dell'Italia alla 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[6].

3. La sfida più impegnativa su cui si concentra quest'ultima ultima edizione del Manuale deriva tuttavia dal fenomeno che maggiormente ha trasformato l'ambiente digitale (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 online globali, la cui azione è divenuta peraltro negli anni sempre meno "passiva". Quella "galassia" di contenuti, che rappresenta una ricchezza per la circolazione delle idee e per la libertà e pluralità dell'informazione, ha finito dunque per essere in qualche modo oggi "gestita" in via prioritaria, appunto, da poche piattaforme online globali.

La sfida per il costituzionalismo è dunque quella di cambiare il paradigma attraverso cui si era soliti guardare alla dimensione digitale nel quale si esplica la libertà di manifestazione del pensiero in Rete, passandosi da una connotazione eminentemente pubblicistica ad una di natura anche privatistica, in quanto la dimensione digitale vede ormai protagoniste le piattaforme online: «spazi formalmente privati», come è stato detto, «che, però, sono entrati prepotentemente a far parte della sfera pubblica»[7]. In altre parole, con l'avvento delle piattaforme online globali, la libertà di espressione in Rete non si svolge più nella tradizionale dimensione verticale (Stato/cittadino) ma in una dimensione triangolare, in cui il terzo protagonista è costituito, appunto, dalle piattaforme online che sono poteri privati[8].

Non è però solo una questione di condivisione della dimensione digitale tra più attori. Più specificamente, si deve tenere conto del fatto che le piattaforme online spesso non svolgono infatti più un ruolo meramente neutrale rispetto al contenuto veicolato in Rete, anche solo in termini di organizzazione dello stesso.

Alcuni Autori, in un'ottica garantistica, hanno guardato alle piattaforme online quali "soggetti" o quale "spazio", assimilandole quindi, rispettivamente, alle formazioni sociali (art. 2 Cost.)[9] o ai luoghi aperti al pubblico (art. 17 Cost.)[10]. L'approccio che è sembrato preferibile accogliere nell'ultima edizione del Manuale è stato quello di guardare alle piattaforme online nell'ottica delle reti di comunicazione elettronica e dei soggetti che "agiscono" su di esse (approccio che rispecchia d'altronde l'impianto che caratterizza il Manuale stesso). In altre parole, si è scelto di guardare a tali fenomeni nell'ottica dell'art. 15 e 21 Cost. e del principio del pluralismo che deve caratterizzare il dispiegarsi di tali libertà attraverso le reti.

Questo, peraltro, nell'ambito di quella più ampia prospettiva giuridica che si è gradualmente affermata in dottrina e nel diritto positivo (quantomeno europeo[11]): quella del costituzionalismo digitale, inteso come "ideologia" volta a limitare i poteri privati sulla Rete (ormai entrati però a far parte della sfera pubblica); così come a partire dal Diciottesimo secolo il costituzionalismo è volto,

6. Cfr. art. 4-*bis*, d.l. 7 ottobre 2020, n. 125, convertito con modificazioni in legge 27 novembre 2020, n. 159.
7. Cfr. Bassini 2019, p. 15 nonché p. 108 ss. Cfr. anche Pollicino-De Gregorio 2021, p. 6.
8. Cfr. Balkin 2018, p. 2011 ss.
9. Sulla possibile qualificazione della comunità di tutti gli utenti di Internet come formazione sociale, cfr. Passaglia 2014, p. 37 ss. Sulla qualificazione dei social networks come formazioni sociali, cfr. Allegri 2018, p. 29 ss.
10. Ancora, cfr. Allegri 2018, p. 44 ss.
11. Sulle profonde differenze con il modo in cui, alla luce del Primo emendamento, il costituzionalismo statunitense ricostruisce la libertà di manifestazione del pensiero e, segnatamente, la sua estrinsecazione nell'ecosistema digitale, cfr. Bassini 2019, p. 176 ss. e p. 217 ss.

nel mondo "reale", a limitare (specie ma non solo) i poteri pubblici[12].

4. Dal punto di vista della regolamentazione giuridica, questo implica un intervento su due versanti.

4.1. In primo luogo, sorge l'esigenza di introdurre strumenti di autoregolamentazione o coregolamentazione per contrastare fenomeni quali la c.d. disinformazione, il discorso d'odio o i contenuti illeciti o nocivi per i minori, che transitano in Rete. La trasformazione delle piattaforme online 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[13] ed alla normativa interna di attuazione del 2003[14].

Nell'ultimo ventennio la difficile opera di sussunzione di nuove e multiformi fattispecie concrete emergenti da tale quadro tecnologico in evoluzione è stata affidata alla soluzione giurisprudenziale, specie da parte della Corte di giustizia dell'Unione 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, *Google LLC*, 2019, *Frank Peterson*, 2021, *TU*, 2022) e della Corte europea dei diritti dell'uomo (*Delfi*, 2015, *MTE*, 2016, *Sanchez*, 2021).

Più di recente l'Unione europea è però finalmente intervenuta a livello di adeguamento normativo alla nuova realtà, introducendosi: una disciplina di carattere generale dei prestatori di servizi intermediari e, segnatamente, dei prestatori di servizi di memorizzazione di informazioni (comprese le piattaforme online) nel regolamento europeo sui servizi digitali (2022)[15]; una disciplina delle piattaforme di condivisione video nella nuova direttiva sui servizi di media audiovisivi (2018)[16]; una disciplina dei servizi di condivisione online nella direttiva sul diritto d'autore nel mercato unico digitale (2019)[17]. Questi ultimi due atti sono stati recepiti dall'Italia, rispettivamente con il d.lgs. di modifica al testo unico dei servizi di media audiovisivi (2021)[18] e con il d.lgs. in materia di diritto d'autore nel mercato unico digitale (2021)[19]. Il tratto distintivo di tali discipline è stato quello di introdurre una serie di obblighi tecnico-organizzativi (sostanzialmente: di moderazione dei contenuti) in capo ai prestatori di servizi di intermediazione, segnatamente le piattaforme online.

12. Cfr., sia pure con diverse sfumature, Celeste 2023, p. 76 ss., De Gregorio 2022, p. 4 ss. e Pollicino 2021, p. 2.
13. Cfr. direttiva 2000/21/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").
14. Cfr. d.lgs. 9 aprile 2003, n. 70, "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".
15. Cfr. regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE ("Regolamento sui servizi digitali").
16. 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.
17. 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.
18. Cfr. d.lgs. 8 novembre 2021, n. 208, "Attuazione della 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, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato".
19. Cfr. d.lgs. 8 novembre 2021, n. 177, "Attuazione della 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".

In questa edizione del Manuale ci si è soffermati in particolare ad esaminare le controverse questioni di diritto costituzionale che tuttavia tali discipline sollevano.

La prima riguarda la restrizione della libertà di espressione discendente dall'imposizione di obblighi tecnico-organizzativi in capo ai prestatori di servizi di intermediazione. Questione che però, quantomeno con riguardo al caso concreto, è stata ritenuta dalla Corte di giustizia non inficiare la legittimità della restrizione stessa[20].

La seconda concerne i rischi di censura privata che potrebbero derivare dall'attribuzione a soggetti privati, quali le piattaforme online, di tali compiti di moderazione dei contenuti[21]. Nell'ultima edizione del Manuale, in primo luogo si individua nella co-regolamentazione delle piattaforme la strada da percorrere, come preferibile a quella della auto-regolamentazione, proprio a fronte di tali rischi. In secondo luogo, una volta constatato come sia inevitabile che le piattaforme online svolgano tale ruolo "censorio" (se pur, finalmente, regolamentato), si conclude come ciò che a questo punto appare indispensabile è che la stessa esistenza delle piattaforme online sia ispirata al rispetto dei principi di pluralismo e concorrenza; e che sia regolamentato il ricorso all'intelligenza artificiale utilizzata dalle piattaforme online (per quanto qui interessa) per rimuovere i contenuti online.

4.2. Ecco allora che il principio del pluralismo torna nuovamente centrale, a fronte dell'ingresso nella sfera pubblica di piattaforme online globali, il cui ruolo rischia di formare nuovi "colli di bottiglia" nel sistema integrato delle comunicazioni e nel mercato unico digitale.

Un principio che deve però essere declinato financo su scala (quantomeno) europea, data la dimensione globale dei fenomeni interessati. E che deve essere "congegnato" in modo più comprensivo: abbracciandosi cioè il sistema integrato delle comunicazioni (come si prefigge di fare oggi, attraverso modalità tuttavia ancora discutibili, l'art. 51 del testo unico dei servizi media audiovisivi, nella versione introdotta nel 2021[22]) ed il mercato unico digitale (oggetto del regolamento europeo sui mercati digitali del 2022[23]); coinvolgendosi la dimensione dei contenuti che transitano "sopra" le reti (si pensi alla propaganda politica, ai servizi di media audiovisivi di interesse generale o comunque ai contenuti mediatici fruibili attraverso le piattaforme online, queste ultime ormai punti di accesso prevalente ai primi); regolamentandosi la dimensione dell'accesso alle reti stesse, prima fra tutte la rete Internet, in termini di neutralità della rete e di servizio universale (è in tali termini, d'altronde, che il codice delle comunicazioni elettroniche del 2021 configura l'adeguato servizio di accesso ad Internet a banda larga a prezzo accessibile[24]).

5. Le sfide che oggi il nostro Paese deve affrontare in questo settore e nella prospettiva del pluralismo sono due.

In primo luogo, occorre risolvere strutturalmente alcuni tradizionali nodi irrisolti del sistema dell'informazione: il conflitto di interessi; la mancanza di una seria normativa a tutela del pluralismo che meglio risponda alle indicazioni della Corte di giustizia nel caso Vivendi; la necessità di codificare e aggiornare la normativa in materia di comunicazione politica e pluralismo informativo; il carente grado di indipendenza dell'Agcom.

In secondo luogo, in un'ottica ormai europea, vi è la necessità di raffinare gli strumenti (introdotti a livello legislativo) a tutela del pluralismo, come si prefigge di fare la proposta di regolamento della

20. Cfr. Corte di giustizia (Grande sezione), sentenza 26 aprile 2022, C-401/19, *Polonia c. Parlamento europeo e Consiglio dell'Unione europea*, paragrafo 39 ss.
21. In generale, nel dibattito statunitense, cfr. Balkin 1999, p. 2295 ss. In Italia, cfr. Grandinetti 2022, specie p. 241 ss., Bassini 2019, p. 111 e Monti 2019, p. 35 ss.
22. Cfr. *supra* nota 18.
23. Cfr. regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 ("Regolamento sui mercati digitali").
24. Cfr. d.lgs. 8 novembre 2021, n. 207, "Attuazione della direttiva (UE) 2018/1972 del Parlamento e del Consiglio dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione)".

Commissione europea recante *legge europea sulla libertà dei media* del 2022[25].

L'auspicio è che l'edizione 2023 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.

Riferimenti bibliografici

M.R. Allegri (2018), *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2018

J. Balkin (1999), *Free Speech and Hostile Environments*, in "Columbia Law Review", vol. 99, 1999, n. 8

M. Bassini (2019), *Internet e libertà d'espressione. Prospettive costituzionali e sovranazionali*, Aracne, 2019

R. Carlini, M. Trevisan, E. Brogi (2022), *Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the years 2021. Country report: Italy*, Fiesole, European University Institute, 2022

E. Celeste (2023), *Digital Constitutionalism. The role of Internet bills of rights*, Routledge, 2023

Commissione europea (2022), *Relazione sullo Stato di diritto 2022. Capitolo sulla situazione dello Stato di diritto in Italia*, 13 luglio 2022

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

O. Grandinetti (2022), *Le piattaforme digitali come "poteri privati" e la censura online*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022

M. Monti (2019), *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in "Rivista italiana di informatica e diritto", 2019, n. 1

P. Passaglia (2014), *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò, P. Passaglia (a cura di), "Internet e Costituzione", Giappichelli, 2014

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

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

25. Cfr. Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno COM/2022/457 final ("Legge europea per la libertà dei media") e modifica la direttiva 2010/13/UE COM(2022) 457 final.

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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0113 • articolo non sottoposto a peer review • pubblicato in anteprima il 21 set. 2023

Marco Bombardelli

Recensione a: Benedetto Ponti, *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità,* Milano, Franco Angeli, 2023

L'Autore è professore ordinario di Diritto amministrativo presso l'Università di Trento

Il libro di Benedetto Ponti considera in modo approfondito l'impatto della disciplina in materia di tutela dei dati personali sull'attività di svolgimento di compiti di interesse pubblico, con lo scopo di individuare i profili di liceità dell'uso di questi dati in tale ambito.

L'Autore muove dalla constatazione di come i trattamenti operati nell'assolvimento dei suddetti compiti rientrino negli spazi di differenziazione che la fonte oggi prevalente in materia – ovvero il Regolamento (UE) n. 2016/679 (GDPR) – lascia ancora alla legislazione nazionale. Spazi che segnalano la peculiarità dell'ambito a cui si riferiscono, essendo invece il GDPR stato adottato proprio per assicurare una disciplina uniforme a livello eurounitario del trattamento dei dati personali, al fine di ridurre quei margini ampi e generalizzati di differenziazione che la precedente direttiva aveva lasciato aperti agli Stati membri, determinando conseguenze negative sia sulla tutela effettiva dei diritti e delle libertà degli individui, sia sulla corretta circolazione dei dati e sulla connessa promozione delle condizioni per lo sviluppo del mercato unico.

In particolare, il GDPR introduce direttamente una base giuridica sufficiente per consentire il trattamento dei dati personali nell'esercizio di funzioni pubbliche, prevedendo all'art. 6, par. 1, lett. e) i presupposti e le condizioni di liceità ad esso corrispondenti. Ma al tempo stesso lascia aperta la possibilità che il legislatore nazionale intervenga per arricchire questi presupposti e queste condizioni, con un proprio intervento, anche di tipo restrittivo. L'Autore attribuisce in parte questa apertura a una tradizione di *deference* della normativa comunitaria rispetto ai legislatori nazionali quando sono in gioco la disciplina dell'attività e dell'organizzazione amministrativa, ma osserva come la stessa si riveli necessaria anche in relazione alle specificità di questo trattamento e in particolare delle modalità di determinazione delle finalità per cui esso può essere operato, che per i poteri pubblici sono individuate in base al principio di legalità, in modo sicuramente diverso rispetto a quanto avviene per i titolari privati di trattamenti.

Muovendo dalla considerazione di questo assetto normativo, Ponti avanza la sua proposta teorica, introducendo una categoria interpretativa che definisce con la nozione di *dual legality standard*, alla luce della quale si propone di sviluppare una ricostruzione del vigente quadro di disciplina dei trattamenti dei dati personali per l'esercizio dei compiti di interesse pubblico.

L'Autore osserva innanzitutto come il previgente regime giuridico introdotto dalla Direttiva 95/46/CE in riferimento al trattamento di dati personali per finalità di interesse pubblico desse sicuramente rilievo al presupposto di liceità connesso alla clausola di necessarietà del trattamento per il perseguimento della finalità di interesse pubblico e come questa operasse sia come vincolo europeo al legislatore statale, sia come parametro di interpretazione. Ma l'efficacia di tale clausola come presupposto di liceità dipendeva dalla disciplina nazionale di recepimento, certo soggetta ai vincoli della direttiva, ma chiamata a disegnare nel concreto, in ambito nazionale, il regime di trattamento dei dati. Ciò finiva per collocare il legislatore nazionale in un ruolo di *dominus* dello standard legale del trattamento dei dati personali a fini di esercizio di compiti di interesse pubblico, standard che quindi risultava essere unico perché in definitiva delineato nella legislazione nazionale, sia pure sotto il regime della direttiva.

Il GDPR, mirando a eliminare la frammentazione delle discipline nazionali conseguente alle diversità con cui gli Stati membri avevano recepito la direttiva, determina il superamento di questa primazia. Pur richiamando (art. 6, par. 1, lett. e), in termini praticamente analoghi a quanto faceva la direttiva (art. 7, lett. e), la necessità del trattamento per l'esecuzione di un compito di interesse

pubblico o l'esercizio di pubblici poteri, il GDPR non richiede che il requisito di necessità del trattamento sia tradotto in disposizioni legislative interne, ma, in virtù della sua natura di Regolamento, lo rende direttamente efficace. Ciò fa sì che l'autorizzazione del trattamento necessario per l'esecuzione di compiti di interesse pubblico non dipenda più dalle previsioni legislative dell'ordinamento interno, ma direttamente delle disposizioni del Regolamento.

L'Autore osserva come questo produca una significativa modifica nel rapporto tra l'operatività della clausola di necessarietà e il principio di legalità. Mentre infatti quest'ultimo impone che il potere sia conferito secondo modalità tipiche per quanto riguarda la tipologia del potere conferito, le forme in cui può essere esercitato e le limitazioni della sfera giuridica che può determinare, nel caso del trattamento dei dati personali ciò che rileva per la liceità del trattamento non sono tanto questi aspetti, non è l'esplicita attribuzione del potere, ma «l'attitudine del trattamento in questione (quali che ne siano le forme, le qualità, le modalità) a consentire il conseguimento di una determinata finalità, secondo un nesso di strumentalità declinato nei termini della *necessarietà*». Ponti ravvisa così come il modo con cui la clausola della necessarietà assegna il potere ricalchi da vicino lo schema finalistico proprio di un potere implicito e si interroga sulla possibilità di inquadrare la clausola di necessarietà entro le coordinate di questo tipo di potere. Ma dopo una attenta analisi ravvisa un disallineamento tra i criteri di legittimazione del trattamento dei dati personali ai fini dell'esercizio dei compiti di interesse pubblico, così come identificati nel GDPR, e i criteri di ammissibilità dei poteri impliciti alla luce del principio di legalità, come declinati dalla giurisprudenza amministrativa nazionale.

È anche in ragione di questo disallineamento che l'A. ritiene necessario introdurre una nuova prospettiva di lettura del fenomeno, che appunto viene imperniata sul duplice standard di legalità. Questa lettura viene impostata da Ponti a partire da due considerazioni, una di carattere storico-positivo e l'altra di carattere sistematico-applicativo. In base alla prima, viene rilevata una concomitanza, e una conseguente esigenza di trovare un punto di equilibrio, tra, da un lato, il parametro di legalità elaborato dal legislatore nazionale a partire dal diritto europeo, e, dall'altro, lo standard legale previsto dal GDPR e idoneo a trovare immediata applicazione negli stessi ordinamenti nazionali nell'ambito di un disegno di progressiva uniformazione. In base invece alla seconda considerazione viene osservato come, anche nella disciplina dettata dal GDPR, a una netta e rigida uniformazione dei presupposti di liceità di trattamento dei dati personali per l'esecuzione di compiti di interesse pubblico, si sia preferita la presa d'atto della molteplicità di approcci regolatori differenziati sviluppatasi negli ordinamenti nazionali, riconoscendo agli Stati membri la facoltà – anche se non l'obbligo – di delineare e modulare il proprio standard, nell'ambito di margini di adattamento riconosciuti dallo stesso Regolamento.

Ponti passa quindi ad esaminare nel dettaglio i due standard legali. Dapprima si sofferma sulla clausola di necessarietà, individuata come standard uniforme/residuale. Questa viene considerata in modo approfondito e sotto vari profili, soffermandosi su questioni come quella relative all'individuazione della base giuridica del trattamento, secondo quanto previsto dall'art. 6, par. 3 del GDPR; quella relativa al principio di limitazione della finalità del trattamento; quella – svolta anche alla luce della giurisprudenza della Corte di giustizia europea – relativa alla definizione del carattere di necessarietà che deve contraddistinguere il nesso di strumentalità che connette il trattamento dei dati personali con l'esecuzione di un compito di interesse pubblico o con l'esercizio di pubblici poteri di cui sia investito il titolare del trattamento.

In questa sua analisi l'Autore affronta e mette in luce molte questioni rilevanti relative al trattamento dei dati personali operato per l'esecuzione di compiti di interesse pubblico. Fra queste quella relativa alle contraddizioni che emergono, e devono essere superate, quando l'applicazione delle norme poste a tutela dei dati personali interferisce con il quadro normativo altrettanto rilevante che prevede «un uso strategico, sistematico ed integrato delle banche dati pubbliche»; quella relativa alla relazione che deve essere individuata tra necessità del trattamento ed efficacia nello svolgimento dei compiti pubblici; quella relativa alla proporzionalità che deve sempre essere assicurata tra l'ampiezza della limitazione sofferta dalla tutela dei dati personali – specie in relazione alla quantità dei dati trattati e alle modalità di comunicazione

e diffusione degli stessi – e quella del margine di manovra riconosciuto all'amministrazione «nel *desumere* in modo *implicito*, alla stregua del solo criterio della *strumentalità necessaria*, i trattamenti lecitamente realizzabili».

Operata quindi l'analisi dello standard uniforme, Ponti passa a considerare questo margine di manovra, da cui deriva la definizione da parte dei legislatori nazionali di standard legali ulteriori, che nella ricostruzione dell'Autore vanno a definire il secondo polo del *dual legality standard*.

Viene esaminata in primo luogo la questione dell'ampiezza attribuibile a questo margine, per la quale Ponti nota come possano essere individuate due diverse estensioni. Si può cioè considerare lo stesso come uno spazio in cui il legislatore nazionale può solo ampliare o completare il quadro dei presupposti e delle condizioni deducibili dallo standard legale definito dal GDPR, che dunque va considerato come una soglia minima sotto cui non è possibile scendere. Oppure si può intendere l'adattamento come «adeguamento», ammettendo anche la possibilità di adottare misure idonee a derogare *in peius* il livello di garanzia stabilito dalla corrispondente disciplina del GDPR. L'Autore ritiene preferibile la prima impostazione, ma osserva come il quadro effettivo delle concrete scelte operate dagli Stati membri nell'utilizzo dei margini di manovra concessi, e in generale delle oggettive condizioni di contesto, contenga anche segnali che vanno nella direzione opposta.

Ponti passa quindi all'esame degli ordinamenti di alcuni Stati europei, volta a verificare come il margine di adattamento previsto dal GDPR sia stato effettivamente utilizzato. Viene rilevato come le discipline effettivamente adottate in materia di trattamento dei dati personali nell'esercizio di compiti di interesse pubblico seguano essenzialmente due schemi. Sono cioè individuabili normative interne *verticali*, che disciplinano, spesso con alto grado di dettaglio, il trattamento dei dati personali nell'esercizio di funzioni specifiche o compiti determinati, e normative interne di carattere *trasversale*, che invece, con previsioni più generali e meno dettagliate, risultano applicabili a intere classi di funzioni pubbliche. L'Autore concentra l'analisi su questo secondo tipo di normative e mette in rilievo, da un lato, come dai casi considerati emerga la presenza di stili regolatori disomogenei nell'utilizzo dei margini di adattamento, indice di un perdurante rilievo degli standard nazionali accanto a quello dettato dal GDPR, e, dall'altro, che le integrazioni introdotte a livello nazionale al *legal standard* del GDPR vanno generalmente nel senso dell'alleggerimento di alcuni dei vincoli derivanti dal Regolamento europeo. Ponti giunge così alla conclusione che le scelte operate dai legislatori nazionali si presentano come regimi regolatori di carattere «composito e modulare» e, nel concreto, confermano l'ipotesi interpretativa del *dual legality standard*.

Ottenuta questa prima convalida della tesi sostenuta, l'Autore passa quindi a considerare in modo più specifico l'ordinamento italiano, richiamando la disciplina nazionale di recepimento della direttiva 95/46/CE nella parte in cui questa dedicava alcuni specifici articoli ai trattamenti effettuati dai soggetti pubblici e poi soffermandosi sui cambiamenti intervenuti a seguito dell'entrata in vigore del GDPR.

Questi vengono a loro volta considerati nelle due diverse fasi in cui finora si sono realizzati. Una prima fase, seguita all'emanazione del d.lgs. 101/2018, in cui il legislatore italiano ha utilizzato i margini di manovra secondo una direzione di «netto irrigidimento» – rispetto sia alla disciplina interna precedente, sia allo standard legale del GDPR – dei presupposti per il trattamento dei dati personali nello svolgimento di compiti di interesse pubblico. Ponti sottolinea al riguardo come in questa fase, anche in base all'interpretazione restrittiva che il Garante ha dato della nuova normativa introdotta, «il *dual legality standard* prende corpo mediante una quasi integrale sostituzione (dei termini oggettivi) del regime del GDPR – modulato sulla *necessary clause* – con uno standard legale caratterizzato piuttosto in termini di *strict legality*». Una seconda fase – innescata anche dall'esigenza di superare alcune rilevanti difficoltà che l'approccio restrittivo ora descritto ha determinato in ambiti importanti di cura dell'interesse pubblico, come il contrasto della crisi sanitaria da Covid 19 o la gestione delle banche dati pubbliche – che con le modifiche normative introdotte dal d.lgs. n. 139/2021 vede introdurre una serie di misure tutte rivolte a rendere più agevole l'uso dei dati personali nello svolgimento di compiti di interesse pubblico.

Ponti individua nel passaggio tra le due fasi una modifica nell'impostazione dello standard legale adottato nel nostro ordinamento, che «smette di caratterizzarsi nei termini della *stretta legalità*» e

«risponde invece in modo del tutto fedele al modello della *necessary clause*». L'Autore ritiene questo passaggio particolarmente rilevante e svolge in relazione ad esso alcune importanti considerazioni. Innanzitutto, sgombra il campo dall'equivoco per cui questa modifica nella configurazione dello standard legale potrebbe portate a una diminuzione della tutela dei dati personali. Viene infatti chiarito che anche nella nuova disciplina introdotta con il «decreto capienze» rimane affidato alla legge il compito di individuare le finalità generali e i compiti di interesse pubblico e rimangono fermi, ed anzi vengono accresciuti, i presupporti per il rispetto del principio di trasparenza del trattamento; dei requisiti di chiarezza, precisione, e prevedibilità di applicazione fissati al considerando (41) del GDPR; del principio di responsabilizzazione del titolare di cui all'art. 5, par. 2 dello stesso Regolamento; delle esigenze di tutela, soddisfatte sia con la previsione di verifiche da parte dell'autorità nazionale di controllo, sia con la precisazione del punto di riferimento per l'attivazione della tutela giurisdizionale.

Poi, osserva che il passaggio a uno standard legale riconducibile alla *necessary clause* contribuisce a migliorare la capacità dell'amministrazione nell'assolvimento dei compiti di cura dell'interesse pubblico, favorendo, da un lato, l'autonomia operativa, l'efficacia e l'efficienza dei titolari del trattamento nello svolgimento dei compiti di interesse pubblico ad essi assegnati e, dall'altro, un migliore coordinamento tra i diversi soggetti pubblici, reso possibile dalla riduzione delle barriere prima frapposte alla circolazione tra di essi dei dati personali comuni e all'integrazione delle banche dati pubbliche.

L'Autore sviluppa poi ulteriormente queste sue considerazioni e si sofferma su tre casi di studio particolarmente significativi per il passaggio dalla prima alla seconda fase di attuazione del GDPR in Italia, riguardanti in particolare gli interventi di lotta alla corruzione nella pubblica amministrazione, il contrasto dell'evasione fiscale e la gestione delle visite medico-fiscali da parte dell'INPS. L'analisi riprende e conferma le considerazioni prima richiamate, mettendo in luce come l'opzione per l'uno o per l'altro dei modelli regolatori oggetto dello studio conduca a profonde differenze sia nel modo di operare che nel ruolo che l'amministrazione assume nello svolgimento dei compiti di interesse pubblico.

Viene così sottolineato come il riferimento alla clausola di necessarietà del trattamento aumenti lo spazio di iniziativa effettivamente assegnato all'amministrazione titolare del trattamento, sia valorizzando il suo ruolo di guida dei processi di innovazione organizzativa e operativa delle funzioni e dei servizi gestiti, sia migliorando la sua capacità di interlocuzione nel rapporto con l'ambiente esterno e in particolare con i fornitori degli apparati hardware e software mediante cui si realizza in pratica il trattamento dei dati. In questo contesto l'Autore sottolinea anche come tale assetto, proprio nella misura in cui assegna una maggiore autonomia operativa e di iniziativa, comporti anche maggiore responsabilità, e sia quindi una sfida per le amministrazioni che intendano approfittarne.

Ponti ricava poi dalla sua analisi anche ulteriori interessanti e non scontate notazioni, sotto il profilo della effettività della tutela dei dati personali. L'Autore infatti, da un lato, osserva come sotto le condizioni della *necessary clause* la presa del principio di limitazione della finalità del trattamento sia più forte, perché rimuove la possibilità che la legge operi come "schermo" degli elementi oggetto di legificazione da un più approfondito esame/sindacato alla stregua del principio di necessarietà e consenta, autorizzandoli espressamente, di derogare al divieto di trattamenti successivi di per sé incompatibili con la finalità originaria di raccolta dei dati. Dall'altro, evidenzia come il fatto che la disciplina del trattamento sia operata non solo con legge ma anche con atto ammnistrativo generale finisce per aumentarne lo spazio di sindacabilità e di raffrontabilità con il parametro costituito dal GDPR.

Ponti conclude quindi la sua analisi soffermandosi sulle implicazioni che l'introduzione *dual legality standard* viene ad avere sulla portata del principio di legalità. In primo luogo, legge la effettiva vigenza della *necessary clause* come una concreta manifestazione di una crisi della legalità, intesa in senso formale, come esclusivo criterio di legittimazione del potere amministrativo. Poi, sottolinea come l'adozione di questo standard legale, nella misura in alleggerisce e semplifica i presupposti di liceità del trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, dia un peso più rilevante, come criteri di legittimazione dell'amministrazione, alle esigenze di funzionalità e buon andamento rispetto a quelle di rispetto della predeterminazione formale in legge della

funzione amministrativa. Ancora, e più in generale, l'analisi svolta conduce l'Autore ad interrogarsi, con riflessioni che paiono sicuramente interessanti e da sviluppare, sulla nozione stessa di legalità, che oltre che misura della corrispondenza degli atti di esercizio del potere (sentenze o provvedimenti) alla sostanza della legge andrebbe letta anche in una ulteriore dimensione di conformità allo scopo.

Il libro di Ponti, con un'impostazione originale e convincente, offre quindi una prospettiva nuova e interessante per la lettura delle disposizioni in materia di tutela dei dati personali nei trattamenti operati nello svolgimento di compiti di interesse pubblico. La sua lettura consente effettivamente di individuare, secondo quanto l'Autore si era prefisso di fare con l'introduzione della categoria del *dual legality standard*, delle coordinate dommatiche utili a tratteggiare i caratteri e le dinamiche della legalità, per come questa si presenta con riferimento al suddetto tipo di trattamenti. Al contempo, offre alle pubbliche amministrazioni delle indicazioni utili per un uso corretto ed efficace dei margini di adattamento che il Regolamento ha reso disponibili, tale fra l'altro da dare concretezza alle previsioni relative alla *privacy by design* (art. 25 del GDPR) e al principio di *accountability* del titolare (art. 5, par. 2 e art. 24 del GDPR). Appare particolarmente condivisibile, a quest'ultimo riguardo, il collegamento finale che l'Autore individua tra l'affermazione dello standard legale della *necessary clause*, la possibilità di "assecondare un rinnovato protagonismo del settore pubblico" e, trattandosi di "uno standard esigente e impegnativo", la necessità che "si torni a investire in modo consistente e appropriato in amministrazioni forti, motivate, innovative e protagoniste, nel governo della società".

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

Autori del 2023

Enrico Albanesi professore associato di Diritto costituzionale presso il Dipartimento di giurisprudenza dell'Università di Genova • **Filippo Bagni** dottorando in Cybersecurity presso la Scuola IMT Alti Studi Lucca • **Mauro Barberio** avvocato amministrativista abilitato presso le magistrature superiori • **Irene Benedetto** dottoranda di ricerca presso il Politecnico di Torino • **Giampaolo Berni Ferretti** avvocato iscritto all'Ordine degli Avvocati di Milano e presidente dell'associazione culturale senza scopo di lucro "Milano Vapore" • **Andrea Bolioli** ricercatore presso MAIZE srl • **Marco Bombardelli** professore ordinario di Diritto amministrativo presso l'Università di Trento • **Carlo Botrugno** ricercatore a tempo determinato presso il Dipartimento di scienze giuridiche dell'Università di Firenze e coordinatore della "Research Unit on Everyday Bioethics and Ethics of Science" presso il Centro di ricerca inter-universitario L'Altro Diritto • **Gabriele Braccioni** avvocato del foro di Urbino; si occupa di diritto delle nuove tecnologie • **Paolo Caldarone** praticante avvocato e tirocinante ex art. 73 DL 69/2013 presso la Procura Generale della Corte Suprema di Cassazione • **Simone Calzolaio** professore associato di Diritto costituzionale presso l'Università degli Studi di Macerata • **Roberto Caso** professore associato di Diritto privato comparato presso l'Università degli Studi di Trento • **Manola Cherubini** ricercatore dell'IGSG-CNR • **Pier Giorgio Chiara** assegnista di ricerca in "Informatica giuridica" presso l'Università di Bologna • **Edoardo Colzani** avvocato, dottore di ricerca in Filosofia del diritto, assegnista di ricerca presso il Dipartimento di giurisprudenza dell'Università di Milano Bicocca • **Angela Cossiri** professore associato di Diritto costituzionale presso l'Università degli Studi di Macerata • **Elia Cremona** assegnista di ricerca in Diritto costituzionale nell'Università degli Studi di Siena • **Deborah De Angelis** avvocato cassazionista del Foro di Roma e direttrice del capitolo italiano di Creative Commons • **Nazareno De Francesco** ricercatore presso MAIZE srl • **Arturo Di Corinto** public affairs and communication advisor presso l'Agenzia per la cybersicurezza nazionale (ACN) e afferisce al Dipartimento di comunicazione e ricerca sociale di Sapienza – Università di Roma • **Massimo Farina** ricercatore (con abilitazione scientifica nazionale al ruolo di professore associato) di Informatica giuridica presso il DIEE - Dipartimento di Ingegneria elettrica ed elettronica dell'Università degli Studi di Cagliari • **Sebastiano Faro** dirigente di ricerca dell'IGSG-CNR • **Christophe Geiger** professore di Diritto presso l'Università Luiss Guido Carli di Roma • **Bernd Justin Jütte** professore associato di Diritto della proprietà intellettuale presso lo University College Dublin Sutherland School of Law e ricercatore senior presso la Facoltà di Giurisprudenza della Vytautas Magnus University (Lituania) • **Camilla Lobascio** dottoranda in "Diritto e innovazione" presso l'Università degli Studi di Macerata• **Erik Longo** professore associato di Diritto costituzionale presso l'Università degli Studi di Firenze • **Cristina Manasse** componente del gruppo di ricerca Digital Cultural Heritage di ICOM Italia • **Sofia Marchiafava** avvocato cassazionista, LLM in Comparative Law, docente del Master di II livello in Informatica giuridica, nuove tecnologie e diritto dell'informatica (Dipartimento di scienze giuridiche, Sapienza – Università di Roma) • **Anna Maria Marras** componente del gruppo di ricerca Digital Cultural Heritage di ICOM Italia • **Lorenzo Nannipieri** ricercatore dell'IGSG-CNR • **Sarah Dominique Orlandi** fondatore e coordinatore del gruppo di ricerca Digital Cultural Heritage di ICOM Italia • **Salvatore Orlando** professore ordinario di Diritto privato presso Sapienza – Università di Roma e direttore dell'OGID (Osservatorio Giuridico sull'Innovazione Digitale) • **Iolanda Pensa** presidente di Wikimedia Italia • **Ginevra Peruginelli** primo ricercatore dell'IGSG-CNR • **Francesco Romano** primo ricercatore dell'IGSG-CNR • **Antonio José Sánchez Sáez** catedrático de Derecho administrativo – Universidad de Sevilla • **Federico Serini** dottorando di ricerca in Diritto pubblico, internazionale e comparato presso Sapienza – Università di Roma • **Caterina Sganga** professoressa associata di Diritto privato comparato presso la Scuola Superiore Sant'Anna di Pisa e coordinatrice del progetto H2020 reCreating Europe • **Irene Sigismondi** docente al Master in diritto dell'informatica, Dipartimento di scienze giuridiche – Sapienza Università di Roma; fellow presso il National Center for Technology and Dispute Resolution (NCTDR) – USA • **Francesco Stocchi** dottorando di ricerca in "Diritto pubblico, Diritto pubblico dell'economia e Filosofia del diritto", Università degli Studi di Milano-Bicocca, Dipartimento di Giurisprudenza • **Giancarlo Taddei Elmi** ricercatore emerito associato presso l'IGSG-CNR di Firenze e già docente di Informatica giuridica presso le Università di Firenze, Milano (Statale e Cattolica) e Cagliari • **Alessandro Tedeschi Toschi** ricercatore indipendente • **Stefano Torregiani** assegnista di ricerca presso l'Università degli Studi di Macerata