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

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0181 • articolo sottoposto a peer review • pubblicato in anteprima il 18 dic. 2024


**Elisa Sorrentino – Anna Federica Spagnuolo**

# Cybersecurity e sovranità digitale nella protezione dei dati personali

Con la crescente complessità della tecnologia, la cybersecurity richiede un approccio integrato e multidisciplinare. Sebbene la tecnologia offra numerose opportunità, il suo rapido sviluppo ha introdotto tecniche sempre più invasive che hanno un impatto sia sulla sfera privata sia su quella pubblica. Inizialmente limitate ai sistemi informatici, queste problematiche riguardano ora i diritti fondamentali, la sicurezza delle infrastrutture e la sovranità degli Stati. In risposta ai rischi e alla complessità crescenti, sono necessarie misure legislative più ampie e mirate. In questo contesto, è fondamentale adottare una prospettiva di cybersecurity che trascenda il dominio puramente tecnico, coinvolgendo il discorso giuridico e politico sulla sovranità digitale e la protezione dei dati. L'obiettivo è promuovere una cybersecurity che garantisca la sicurezza dei dati e delle informazioni nel pieno rispetto dei diritti fondamentali sanciti da standard più elevati e universalmente validi.

*Cybersecurity – Sovranità digitale – Dati personali – Diritti fondamentali*

## Cybersecurity and Digital Sovereignty in Personal Data Protection

With the increasing complexity of technology, cybersecurity requires an integrated and multidisciplinary approach. Although technology offers numerous opportunities, its rapid development has introduced increasingly invasive techniques that impact both the private and public spheres. Initially limited to information systems, these issues now affect fundamental rights, infrastructure security, and state sovereignty. In response to growing risks and complexity, broader and more focused legislative measures are needed. In this context, it is crucial to adopt a cybersecurity perspective that transcends the purely technical domain, engaging the legal and political discourse on digital sovereignty and data protection. The goal is to promote cybersecurity that ensures data and information security while fully respecting fundamental rights enshrined in higher and universally valid standards.

*Cybersecurity – Digital Sovereignty – Personal Data – Fundamental Rights*

Le Autrici afferiscono all'Istituto di Informatica e Telematica del CNR, sede di Cosenza

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambe le Autrici ed è stato parzialmente realizzato nell'ambito delle attività del progetto "*SEcurity and RIghts in the CyberSpace – SERICS (PE00000014)*" – Piano Nazionale di Ripresa e Resilienza MUR finanziato dall'Unione europea – NextGenerationEU, CUP B53C22003950001

Un particolare ringraziamento è rivolto al prof. Domenico Talia per aver fornito preziosi consigli e interessanti spunti di riflessione sull'impatto che i modelli predittivi e gli algoritmi di *machine learning* possono avere su decisioni e comportamenti umani

## 1. Introduzione

Per instaurare un clima di fiducia nel complesso e dinamico cyberspace[1], la cybersecurity, considerata la crescente estensione del suo campo d'azione, richiede un approccio multidisciplinare e integrato[2]. Sebbene la tecnologia offra significative opportunità di progresso, miglioramento culturale, sanitario, tecnologico ed economico, il suo sviluppo rapido e pervasivo facilita difatti l'emergere di tecniche e modalità sempre più invasive, incidendo sia sulla vita privata dei cittadini sia sulla sfera dell'attività pubblica.

Le criticità originariamente connesse esclusivamente ai sistemi informatici e alle reti di comunicazione[3] oggi manifestano effetti pervasivi e reticolari, impattando significativamente sui diritti fondamentali e sulle libertà delle persone[4], sugli equilibri politici e sulla sicurezza di infrastrutture, ponendo sfide inedite alla sovranità degli Stati.

Per di più, l'aumento della tipologia dei rischi è accompagnato da una proporzionale crescita degli attori coinvolti e dalla complessità delle tecnologie sviluppate. Questo contesto determina un cambio di paradigma che richiede, da parte del legislatore nazionale e internazionale, risposte molteplici e diversificate.

A questo si aggiunge la proliferazione normativa degli ultimi anni, spesso ancora in fase di attuazione, che ha consolidato un'architettura di sistema estremamente vasta e variegata, generando

1. Martino 2018, p. 66. L'autore 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*.
2. In questo senso il Rapporto CLUSIT (Associazione Italiana per la sicurezza informatica) per l'anno 2016, p. 12 definisce la cybersecurity come «il gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti […] costruite negli anni a partire da esigenze di compliance».
3. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM/2001/0298). Creare una società dell'informazione sicura per l'Ue significa migliorare la sicurezza delle infrastrutture dell'informazione ma anche lotta alla criminalità informatica. Si veda Commissione delle Comunità Europee, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni - *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica (eEurope 2002)*, Bruxelles, 26 gennaio 2001 COM(2000) 890, e la Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni (*Open Network Provision* - ONP).
4. Esposito 2019.

inevitabili difficoltà applicative e onerosi sforzi nel recepimento da parte degli Stati membri.

Uno degli ostacoli più significativi è rappresentato dall'uso di un linguaggio tecnico giuridico settoriale, che crea barriere comunicative e ostacola l'armonizzazione normativa.

La diversità delle esigenze dei vari ordinamenti nazionali rende particolarmente ardua la creazione di un quadro regolatorio euro unitario coeso ed efficace, specialmente in settori altamente specialistici.

Questa difficoltà è particolarmente accentuata nel campo della protezione dei dati personali[5], in cui l'armonizzazione tra le disposizioni sovranazionali e nazionali richiede un'importante fase di interpretazione e coordinamento che non sempre risulta agevole e spesso genera conflitti normativi[6].

Per superare queste sfide, è auspicabile ripartire dal rispetto per la gerarchia delle fonti, valorizzando i trattati internazionali che incorporano principi condivisi e utilizzano un linguaggio universale[7].

Partendo da questo presupposto, con l'intento di facilitare un dialogo più fluido e produttivo tra le politiche interne e quelle sovranazionali, il presente lavoro sottolinea l'importanza cruciale di una concezione di cybersecurity che trascenda il mero confronto tecnico proiettandosi nell'attuale e complesso dibattito giuridico e politico sulla sovranità digitale[8] in relazione alla protezione dei dati personali. L'intento è di offrire una visione di cybersecurity inserita in un contesto di sovranità digitale, la cui legittimazione ultima risiede nella capacità di garantire la sicurezza dei dati[9] e delle informazioni, in piena ottemperanza ai diritti fondamentali sanciti da norme di rango superiore e valide *erga omnes*[10].

5. L'art. 4, paragrafo 1, del Regolamento Generale sulla Protezione dei Dati (GDPR) definisce con «"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Si aggiunga che il Considerando 30 prevede che: «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».
6. Il GDPR impone standard rigorosi per la protezione dei dati personali. Tuttavia, l'applicazione uniforme di tali standard è resa difficile dalle differenti legislazioni nazionali e dalle interpretazioni divergenti delle stesse norme. Questa situazione richiede un'armonizzazione giuridica che spesso risulta conflittuale, con conseguenti difficoltà nell'attuazione di politiche coese.
7. Il Trattato di Lisbona e la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108), rappresentano, a titolo esemplificativo, strumenti normativi fondamentali che offrono un quadro di principi e terminologie condivise a livello internazionale.
8. La sovranità digitale è stata finora definita in modo piuttosto vago. Recentemente è emersa la nozione "Europe's ability to act independently in the digital world". A tal proposito si veda Madiega 2020. Per una panoramica della letteratura in tema di sovranità digitale si rinvia all'analisi di Hummel–Braun–Tretter–Dabrock 2021. Gli autori identificano sei differenti nozioni di sovranità. Sull'argomento si veda, inoltre, Moerel–Timmers 2021; Simoncini 2017, p. 19 ss.
9. Sull'argomento si veda, Orofino 2022, pp. 82 ss., Finocchiaro 2014; Passaglia 2016; Pizzetti 2016, p. 9 ss.
10. Si veda Cassese 2006. Nel testo si legge che: «Le norme […] erga omnes, […] presentano le seguenti caratteristiche: sono obblighi che proteggono valori fondamentali per la comunità internazionale nel suo insieme (pace, diritti umani, autodeterminazione dei popoli, protezione dell'ambiente); sono obblighi di natura solidale, nel senso che essi incombono su ogni membro della società internazionale nei confronti di tutti gli altri membri

Analizzeremo quindi l'evoluzione di una disciplina che, sebbene nata per garantire il corretto funzionamento e l'efficienza delle infrastrutture pubbliche e private, oggi è deputata a preservare l'esercizio dei diritti fondamentali[11] e a favorire uno sviluppo tecnologico sostenibile e rispettoso dei principi democratici[12] in risposta alle esigenze di una società moderna, democratica e partecipata[13].

## 2. Dall'indipendenza del cyberspazio alla sovranità digitale

Nel 1996 la pubblicazione della Dichiarazione di indipendenza del *cyberspazio*[14] fu dettata da un clima di generale entusiasmo per la rapidissima e travolgente rivoluzione digitale in corso. Fu in nome di una più ampia autonomia, di una diffusa libertà di opinione e di espressione, che i padri della rete e i loro giovani allievi «codificarono e scolpirono nella pietra l'antipatia per i governi e per la regolamentazione»[15], disponendo di fatto l'assenza di autorità all'interno di questo ecosistema. Non era stato evidentemente previsto che i potenti del web avrebbero presto iniziato a dominare gli ampi spazi geopolitici[16] traendo grandi vantaggi dallo sviluppo di un *cyberspazio* privo di regole[17], in cui i dati assumono sempre più velocemente il ruolo di fulcro in un nuovo archetipo di capitalismo estrattivo basato sulle piattaforme digitali[18]. Saranno il caso *Snowden*[19] e lo scandalo *Facebook – Cambridge Analytica*[20] a evidenziare il pericolo indotto dall'utilizzo fraudolento dei dati personali degli utenti da parte di piattaforme multinazionali. Due episodi dal forte impatto mediatico che andranno ad agitare il dibattito politico sulla necessità di intervenire in maniera radicale a tutela dei diritti individuali nel contesto digitale garantendo maggiore privacy e sicurezza degli utenti. Il caso *Schrems* e il relativo dispositivo della Corte di Giustizia UE andranno invece a costituire il primo importante passo da un punto di vista giurisprudenziale per l'affermazione di una sovranità digitale dell'Unione europea[21]. La decisione della Corte andrà difatti a ribaltare l'orientamento decisivo nel caso *Google Spain* in cui era diversamente predominante la diffusa convinzione che il trattamento dei dati da parte del grande motore di ricerca, doveva ritenersi

(o, nel caso essi discendano da trattati, nei confronti di tutte le altre parti contraenti); ad essi corrisponde un diritto sostanziale che appartiene ad ogni membro della comunità internazionale (o ad ogni parte al trattato); l'azione a tutela di tale diritto è esercitata per conto dell'intera comunità internazionale o dell'insieme delle parti contraenti) per salvaguardare gli interessi fondamentali di quella comunità».

11. Si veda a tal proposito Rodotà 2006; Pollicino–Bertolini–Lubello 2013.
12. Brighi–Chiara 2021, pp. 11 ss.
13. Si veda a tal proposito Santaniello 2022.
14. Barlow 1996.
15. Bertola 2022.
16. Cfr. Amato Mangiameli–Campagnoli 2020.
17. Mangiameli 2023-a, p. 281. Si veda inoltre Serini 2023, e ancora Walker 2015. Si veda ancora Franzese 2009.
18. Cfr. Harvey 2006; Formenti 2008; Zuboff 2019.
19. Nel 2013, Edward Snowden, ex contractor dell'intelligence degli Stati Uniti, ha divulgato l'esistenza di riservatissimi programmi di sorveglianza globale condotti dall'agenzia governativa National Security Agency (NSA) accendendo un forte dibattito sulla privacy, sulla sorveglianza governativa e sul delicato equilibrio tra sicurezza nazionale e diritti individuali. Si veda a tal proposito Darnis 2021. Lo scandalo Facebook – Cambridge Analytica ha messo in evidenza il pericolo dell'utilizzo fraudolento dei dati personali degli utenti da parte di piattaforme multinazionali. I dati di 87 milioni di utenti, di cui 2,7 milioni si trovano nell'Ue, potrebbero essere stati violati e usati impropriamente. Della vicenda si è occupato anche il Parlamento europeo.
20. Nel 2018 Christopher Wylie rivelò che Cambridge Analytica aveva ottenuto i dati personali degli utenti attraverso accordi con Aleksandr Kogan, creatore di un'app di Facebook che raccoglieva informazioni per scopi di ricerca. Cambridge Analytica ha poi utilizzato questi dati per influenzare e manipolare il voto in eventi chiave come la campagna per il referendum sulla Brexit e le elezioni presidenziali statunitensi del 2016, che hanno visto la vittoria di Donald Trump. Si veda a tal proposito Faini 2019-a; Simoncini 2019.
21. Zeno-Zencovich 2016.

effettuato sui *mainframe* presenti negli Stati Uniti, e quindi non fosse soggetto alla direttiva UE sui dati personali[22]. Inizia, in altri termini, a prendere forma la consapevolezza che sia necessario arginare una pericolosa idea di sovranità digitale mista "sia pubblica che privata" in cui la capacità di regolamentare i mercati e gestire la comunicazione pubblica sia delegata alle grandi multinazionali che forniscono le infrastrutture. Si impone come linea di indirizzo strategica la volontà di invertire quella medesima ambivalenza che rischia di proiettarsi anche sul mondo del diritto, spingendo verso il superamento della classica distinzione pubblico-privato[23]. Dinanzi al timore di ulteriori minacce del tutto inedite[24] si afferma un evocativo concetto di sovranità digitale[25] da intendersi come la capacità di un Paese di esercitare autorità all'interno del *cyberspazio*, garantendo l'indipendenza tecnologica e il controllo sui dati personali. Sarà la Cancelliera tedesca Angela Merkel, nel luglio 2020, a lanciare per la prima volta l'idea di definire la sovranità digitale come tema centrale all'interno del suo programma ufficiale per la presidenza del Consiglio europeo prospettando l'implementazione di un'infrastruttura digitale europea ad alte prestazioni, sovrana e resiliente[26]. Questo è essenzialmente l'obiettivo del progetto europeo *Gaia X*[27], finalizzato a ridurre la dipendenza dalle piattaforme dei cloud extraeuropei[28] e a creare un ecosistema digitale aperto, trasparente e sicuro, in cui dati e servizi possano essere resi disponibili, raccolti e condivisi in un ambiente di fiducia. Lo scopo è quello di rintracciare forme di maggior tutela per l'autodeterminazione dei propri cittadini e delle imprese dinanzi alle sfide poste dall'ampio dispiegamento di tecnologie digitali altamente invasive, come l'intelligenza artificiale e l'"Internet delle cose". Seguirà la progressiva affermazione della sovranità digitale come priorità strategica nell'agenda politica dell'Unione europea. Questo è testimoniato anche dai recenti pronunciamenti di Ursula von der Leyen[29]. La Presidente della Commissione europea, in un'ottica di rinnovato impegno verso la costruzione di un'Europa più verde, digitale e resiliente sottolinea l'esigenza di plasmare un continente in cui i cittadini possano liberamente esprimere la propria identità, coltivare le proprie aspirazioni e relazioni interpersonali, in linea con i principi fondanti delle democrazie liberali[30].

22. *Ibidem*.
23. Simoncini–Cremona 2022, p. 258.
24. Si veda a tal proposito Simoncini 2017.
25. Per una panoramica della letteratura in tema di Sovranità Digitale si rinvia all'analisi di Hummel–Braun–Tretter–Dabrock 2021. Gli autori identificano sei differenti nozioni di sovranità. Sull'argomento si veda, inoltre, Moerel–Timmers 2021; Simoncini 2017. Si veda inoltre Finocchiaro 2022.
26. Dal sito della Presidenza tedesca del Consiglio dell'Unione europea si veda: *Secure and sovereign, European-based, resilient and sustainable digital infrastructure is essential to this transformation*.
27. Il progetto europeo *Gaia X* ha come obiettivo principale la creazione di un'infrastruttura cloud che rafforzi la sovranità digitale, la competitività e il peso politico dell'EU attraverso la creazione di "data space", "spazi di dati" in grado di trasporre in forma digitale gli ecosistemi fisici, naturali, industriali o sociali già esistenti all'interno dell'Unione europea.
28. Si veda a tal proposito Autolitano–Pawlowska 2021 o ancora il Dossier *The Gaia-X Ecosystem - A Sovereign Data Infrastructure for Europe*.
29. La Presidente von der Leyen nella sessione plenaria del Parlamento europeo ha evidenziato come «Nulla di tutto ciò è fine a sé stesso: è in gioco la sovranità digitale dell'Europa, sia su piccola che su larga scala». Per approfondimenti si veda il discorso sullo stato dell'Unione.
30. In questo solco, la Presidente von der Leyen ha delineato una serie di iniziative volte a rafforzare gli elementi costitutivi del Green Deal europeo proiettando l'Unione verso una trasformazione digitale che sia rispettosa dei diritti fondamentali degli individui. Tale approccio si inserisce in una più ampia strategia di democratizzazione e costituzionalizzazione della rete, finalizzata a limitare l'esercizio del potere da parte delle grandi piattaforme digitali e a riaffermare il primato dei valori democratici. Questo orientamento, peraltro, riecheggia le riflessioni già espresse dalla Cancelliera tedesca Angela Merkel, la quale ha sottolineato l'importanza di un

Contestualmente inizia a palesarsi la necessità di arginare l'impatto sempre maggiore delle nuove tecnologie nell'area del diritto, impatto che ha scardinato le coordinate su cui si fondava l'esercizio tradizionale dei pubblici poteri a partire dal principio di territorialità fino alla nozione stessa di sovranità[31].

## 3. La sfida della cybersecurity: protezione dei dati e normative nell'era delle violazioni informatiche

Sono enormi le quantità di dati[32] che ogni giorno vengono generate e raccolte da organizzazioni pubbliche[33] e private. Elaborati, analizzati, condivisi e riutilizzati per estrarne valore prezioso, diventano sempre più spesso un bersaglio ambito per le intrusioni e le violazioni della sicurezza informatica. Per come si evince dal Rapporto 2024 sulla Sicurezza ICT solo in Italia (CLUSIT)[34] gli attacchi cibernetici sono in espansione. Confrontando i dati del 2019 con quelli del 2023 la crescita in termini numerici degli attacchi rilevati da fonti pubbliche è stata del 60% (da 1.667 a 2.779). Nel 2023 gli attacchi sono aumentati dell'11% a livello globale (ma in Italia sono aumentati ben del 65%). È indubbio che ci troviamo di fronte a un incremento esponenziale della superficie di attacco con impatti profondi, duraturi e sistemici su ogni aspetto politico, economico ma anche e soprattutto sociale. È difatti dall'uso improprio e malevolo di dati e in particolare di dati personali che si alimenta quella disparità informatica in cui i diritti fondamentali sono preda del dominio digitale. Così, attraverso una corposa produzione normativa sia il legislatore europeo che il legislatore nazionale[35]

patto intergenerazionale che consenta di plasmare un futuro digitale all'insegna della sostenibilità e dell'equità. In tale prospettiva, la Conferenza sul Futuro dell'Europa rappresenta un'occasione cruciale per rinsaldare i legami tra le istituzioni comunitarie, i cittadini e la società civile, anche attraverso l'utilizzo di innovative piattaforme digitali.

31. De Rosa 2021, p 11. Si veda ancora Gatti 2019.

32. Come riportato nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Una strategia europea per i dati*, COM(2020) 66, 12 febbraio 2020, 2, il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025. È utile considerare anche che i dati e le informazioni aumentano ad una velocità vertiginosa tale da creare un ambiente saturo di dati, in tal senso Galetta 2018, p. 327, riporta alcuni dati inerenti al tema dell'aumento del volume delle informazioni disponibili.

33. Sull'integrazione tra digitalizzazione e data protection si veda Faini 2019.

34. Si veda il Rapporto Clusit 2024.

35. In un quadro di collaborazione europea e internazionale, nel 2013 nel nostro Paese è stata formulata una prima architettura della sicurezza cibernetica nazionale mediante il DPCM del 24 gennaio 2013 (c.d. Decreto Monti). Il DPCM ha delineato «l'architettura istituzionale deputata alla sicurezza nazionale […] con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale» assegnando a questo scopo compiti spesso strettamente complementari a vari attori istituzionali (Presidente del Consiglio dei ministri, Comitato Interministeriale per la Sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza, Nucleo per la Sicurezza Cibernetica) rendendo perciò indispensabile l'instaurarsi di numerose interazioni reciproche tra gli stessi. Il panorama normativo nazionale ha poi subito modifiche nel 2017 con l'emanazione di un nuovo DPCM (c.d. Decreto Gentiloni), che ha delineato i nuovi assetti organizzativi dell'architettura nazionale di cybersecurity e ha introdotto una Strategia nazionale in materia mediante l'adozione del nuovo Piano Nazionale21, che aggiorna i provvedimenti del dicembre 2013. Per il primo intervento di rango primario, invece, si è dovuto attendere il 2018, con l'emanazione del d.lgs. 65/2018 (c.d. d.lgs. NIS). Con questo atto l'Italia, in recepimento della Direttiva NIS, ha rafforzato il proprio quadro normativo in materia di cybersecurity attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica, oltre l'adozione di una Strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei ministri. Al d.lgs. NIS ha fatto seguito il d.l. 21 settembre 2019, n. 105 che ha definito il Perimetro di sicurezza nazionale cibernetica al fine di garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi informatici delle amministrazioni pubbliche nonché degli enti e degli operatori sia pubblici che privati. Sul piano del diritto, pertanto, si riscontra una continua evoluzione

pongono quale obiettivo principale l'idea di perseguire l'interesse comune europeo ad abitare una società protetta nella sua dimensione *onlife*[36] e più resiliente alle minacce cibernetiche. I legislatori nel dettare le norme in materia di protezione dei dati personali, dimostrano una spiccata consapevolezza dell'enorme portata assunta, negli ultimi decenni, dal fenomeno della circolazione dei dati che ha reso le informazioni personali "disponibili al pubblico su scala globale"[37].

In questa prospettiva, nel 2013 la *Cybersecurity Strategy*[38] definisce gli orientamenti generali al fine di rafforzare l'efficienza complessiva dell'Ue. La Strategia, nel delineare i principi su cui è fondato il *cyberspazio*, evidenzia *in primis* il valore dei diritti e delle libertà fondamentali, sottolineando il rapporto sinergico tra *cybersicurezza* e protezione dei dati personali. Nella medesima prospettiva, la Direttiva NIS[39], attuata in Italia solamente nel 2018, rappresenta il primo esempio di normativa orizzontale e, quindi, il primo tentativo di armonizzazione dei livelli di sicurezza dei sistemi informatici. Essa introduce l'obbligo a carico degli Stati membri di provvedere affinché determinati soggetti (operatori di servizi essenziali e fornitori di servizi digitali) notifichino senza indebito ritardo all'autorità competente o al gruppo d'intervento per la sicurezza informatica gli incidenti che abbiano un impatto rilevante rispettivamente sulla continuità dei servizi essenziali prestati o sulla fornitura di un servizio digitale.

Sempre più urgente appare dunque identificare regole, metodologie e strumenti più appropriati e idonei a proteggere i dati da accessi non autorizzati e da attacchi malevoli[40]. In tal senso interviene il Regolamento 2016/679/UE (GDPR) imponendo di trattare i dati personali in modo da garantirne un'adeguata sicurezza e riservatezza, integrità e disponibilità[41]e per impedire l'accesso o l'utilizzo non autorizzato delle informazioni e dei sistemi impiegati per il loro trattamento. In tale contesto la cybersecurity si pone al centro di un ampio e diffuso dibattito sul piano tecnologico, giuridico e politico identificandosi come uno dei pilastri su cui viene (ri)edificato il sistema europeo di protezione dei dati personali[42].

Costruire un ecosistema digitale sicuro richiede l'adozione di standard riconosciuti per garantire

della cornice normativa, a cui si aggiungono il d.l. 14 giugno 2021, n. 82 e alcuni specifici commi della l. 29 dicembre 2022, n. 197. Il d.l. 82/2021 mira a rafforzare le misure a tutela della sicurezza mediante l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), il Comitato interministeriale per la cybersicurezza (CIC) e il Nucleo per la cybersicurezza, al quale è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri in materia di prevenzione di eventuali crisi o attacchi cyber. L'ACN assume la responsabilità di tutelare la sicurezza nazionale, inclusa quella nello spazio cibernetico, e dispone di funzioni di coordinamento tra le altre Autorità competenti nel settore e di predisposizione della Strategia nazionale di cybersicurezza. Al CIC sono attribuite funzioni di sorveglianza sull'attuazione della suddetta Strategia e di supporto alle politiche della Presidenza del Consiglio dei ministri nell'ambito del Perimetro di sicurezza. Infine, al Nucleo per la cybersicurezza è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri nella prevenzione di eventuali crisi o attacchi cyber. I commi da 899 a 902 della legge n. 197/2022 danno attuazione alla Strategia nazionale di cybersicurezza, formalmente adottata mediante DPCM in data 17 maggio 2022, e rendono effettivo il relativo piano di implementazione istituendo nel bilancio del Ministero dell'Economia e delle Finanze specifici fondi.

36. Floridi 2015; Floridi 2009.
37. Regolamento Generale sulla Protezione dei Dati (GDPR) - Considerando 6.
38. Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, Bruxelles, 7 febbraio 2013 JOIN(2013) 1.
39. 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.
40. Flor 2019, p. 5.
41. V. Passaglia 2016; Pizzetti 2016, p. 9 ss. Sull'integrazione tra digitalizzazione e data protection si veda Faini 2019.
42. Flor 2019.

che le soluzioni tecniche utilizzate siano resilienti e che gli utenti possano fidarsi della protezione dei propri dati. Sarà il Regolamento UE 2019/881 (*Cybersecurity Act*)[43] a porre come obiettivo principale quello di rafforzare la resilienza dell'Unione agli attacchi informatici e favorire la c.d. "*security by design*" e il consolidamento di una *cybersecurity culture*[44] fin dagli stadi iniziali della progettazione o della realizzazione dei prodotti e dei servizi tecnologici, in cui sono compresi i dispositivi di consumo connessi alla rete e a quella sua parte c.d. IoT (*Internet of Things*).

Il Regolamento UE 2019/1150[45] rappresenta un fondamentale strumento normativo che si prefigge l'obiettivo di introdurre maggiore equità e trasparenza nelle relazioni contrattuali tra le piattaforme digitali e gli utenti commerciali. Il succitato Regolamento inizia a considerare la crescente dipendenza delle imprese dagli intermediari digitali e a valutare le condizioni svantaggiose che in un rapporto sbilanciato possono derivare per i consumatori finali[46]. In questa direzione la Commissione europea ha più volte sottolineato l'importanza di garantire l'indipendenza digitale dell'Unione europea da potenziali influenze di giurisdizioni straniere e nella comunicazione *Plasmare il futuro digitale dell'Europa 20*[47], evidenzia che le tecnologie digitali devono non solo contribuire al progresso dell'Europa migliorando la vita delle persone e la competitività delle imprese europee, ma anche rispettare i valori fondamentali su cui si basa l'Europa stessa. La Commissione, proprio al fine

43. Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio 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». *In primis* il regolamento, da un lato, definisce genericamente la "cibersicurezza" come l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche; dall'altro lato, adotta una nozione omnicomprensiva di "minaccia informatica", intesa come una qualsiasi circostanza, evento o azione che potrebbe danneggiare, turbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. In secondo luogo, il Cybersecurity Act vuole istituire un quadro europeo di certificazione al fine di migliorare il livello di cybersecurity in Europa, anche attraverso l'armonizzazione dei sistemi europei di certificazione della sicurezza informatica.
44. Riferimenti in tal senso si rinvengono anche nel report pubblicato da ENISA nel 2017: cfr. Enisa 2017, in cui si legge «Cybersecurity Culture (CSC) of Organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies. […] (T)echnologies cannot protect organisations if incorrectly integrated and utilised.» (p. 7 ss.). In un secondo report del 2019 ENISA riprende il difetto di una nozione universale di cybersecurity («there is no universally accepted definition of cybersecurity, with descriptions of the term varying across authors on multiple dimensions, including the nature of what is protected, from whom, and whether or not unintentional actions are included Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity»), concentrandosi su *human aspects of cybersecurity*, dal punto di vista "defending organisations", e "socio-technical perspective". Cfr. Enisa 2019, che parte dai risultati del report Enisa 2016.
45. Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.
46. La proposta attuale si basa sulla constatazione che le grandi piattaforme digitali esercitano un controllo significativo sull'accesso ai mercati digitali, agendo come principali intermediari tra gli utenti finali e le imprese. Grazie alla loro posizione di dominio e alla capacità di profilare dettagliatamente gli utenti, tali piattaforme possono adottare pratiche commerciali che favoriscono la propria posizione a discapito della concorrenza leale. Al fine di promuovere un ambiente di mercato più equo e competitivo, la nuova proposta di regolamento identifica specifici "servizi digitali base" controllati da un numero limitato di grandi piattaforme. Questi servizi comprendono intermediazioni, social network, motori di ricerca e altri, mirando a garantire che le regole siano rispettate in modo da tutelare gli interessi degli utenti commerciali e dei consumatori finali. Si veda a tal proposito Allegri 2021.
47. Commissione europea 2020.

di proteggere l'indipendenza digitale dell'Unione, propone di introdurre nuove regole volte a contrastare comportamenti e contenuti illeciti online, di definire chiaramente le responsabilità dei gestori dei flussi di informazioni e dati, e di aumentare la trasparenza nella gestione delle informazioni su Internet. La Direttiva NIS 2[48], proposta nel dicembre 2020 e entrata in vigore a gennaio 2023, insieme al Regolamento *Cyber Resilience Act* (CRA) rappresentano invece un passo significativo verso la creazione di principi comuni e regole di *policy* sulla cybersecurity per affrontare le crisi causate da diversi livelli di resilienza cibernetica tra gli Stati membri. Riconoscendo la dinamicità e la costante evoluzione delle minacce cibernetiche e la necessità di bilanciare le esigenze della sicurezza informatica, dell'innovazione tecnologica con il rispetto dei diritti dei cittadini sarà il Regolamento 2023/2841[49] a delineare una difesa comune basata su misure orientate ad una resilienza digitale[50] integrata e avanzata. Il Regolamento in vigore dal 1° gennaio 2024 stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione ponendo quale obiettivo principale quello di proteggere i dati e la sovranità digitale degli Stati membri senza ostacolare l'innovazione e la competitività in un mercato digitale sempre più globale e dinamico.

Nonostante la corposa produzione normativa, ad oggi è ancora carente una lettura unitaria di obblighi e doveri e questo determina una disparità di livelli di *cyber* resilienza tra gli Stati membri. Questo scenario inibisce la creazione di un *framework* di *cybersicurezza* coerente, uniforme e soprattutto la capacità di resistere alle pressioni di un mercato sempre più aperto e competitivo. Non è un caso che ad oggi Commissione europea e Agenzia Europea per la Sicurezza Informatica (ENISA) siano al centro di un dibattito sull'*European Cybersecurity Certification Scheme for Cloud Services* (EUCS)[51]. La nuova versione della bozza per la certificazione *cloud* non comprende gli stringenti requisiti di sovranità digitale che caratterizzavano la prima proposta avanzata in adesione al *Cybersecurity Act*[52]. Il progetto di schema di certificazione di sicurezza per i servizi di cloud (EUCS) inizialmente includeva requisiti di sovranità che avrebbero richiesto ai fornitori di servizi di *cloud* di localizzare i dati e le operazioni all'interno dell'Ue. In altre parole, i requisiti di sovranità avrebbero costretto i principali fornitori di *cloud* non Ue come *AWS*, *Google* e *Microsoft* a fare investimenti massicci in infrastrutture di data center locali dedicate, processi di conformità regolamentare e capacità di controllo sovrano per offrire servizi nell'Ue[53]. Il progetto di schema EUCS più recente ha, pertanto, rimosso i requisiti di sovranità al fine di scongiurare il pericolo di limitare la concorrenza, aumentare i costi e frenare l'innovazione[54].

48. 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).
49. Regolamento (Ue, Euratom) 2023/2841 del Parlamento europeo e del Consiglio del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.
50. Quando parliamo di resilienza digitale non parliamo di un ossimoro, ma di un profondo cambio di paradigma. La crisi pandemica, in particolare, ha messo in rilievo l'immagine di una tecnologia digitale frenetica, transitoria, a rapida obsolescenza, fonte di continua innovazione, ma anche in grado di permettere al sistema Paese di resistere, di affrontare l'impatto di eventi imprevedibili o addirittura impensabili.
51. Bozza di proposta dell'*European Cybersecurity Certification Scheme for Cloud Services* (EUCS).
52. In forza del Regolamento (UE) 2019/881, il quadro di certificazione di cybersecurity dell'Ue stabilisce la procedura per la creazione di schemi di certificazione di cybersecurity dell'Ue, che coprono i prodotti, i servizi e i processi ICT. Ogni schema specificherà uno o più livelli di assicurazione (basico, sostanziale o alto), in base al livello di rischio associato all'utilizzo previsto del prodotto, del servizio o del processo.
53. Si vedano a tal proposito gli annunci di alcuni dei principali fornitori di cloud non Ue: *AWS Digital Sovereignty*, *Microsoft Cloud for Sovereignty*.
54. Chee 2024.

## 4. Sovranità digitale e cybersecurity: sinergia a tutela dei diritti nell'era delle crisi globali

Nella contemporanea società del rischio[55] il dibattito sul concetto di sovranità digitale ha come cornice un contesto particolarmente delicato segnato prima dalla pandemia[56] e a seguire dai conflitti bellici[57] che coinvolgono anche i paesi dell'Ue e che pongono enormi interrogativi sui possibili sviluppi in ottica *cyber*.

Le minacce cibernetiche rappresentano difatti un nemico sempre più evoluto e insidioso per l'esercizio dei diritti collettivi ed individuali e la fitta risposta normativa in materia di cybersecurity è prova e testimonianza della tensione esistente. Nondimeno, il concetto di sovranità digitale è ancora essenzialmente inteso come pratica politica discorsiva piuttosto che giuridica normativa[58] generando una situazione di frammentazione globale che esprime la crisi della rappresentazione unitaria del potere[59]. La sovranità digitale, intesa come la capacità di gestire in modo autonomo le tecnologie digitali e le informazioni, rappresenta una sfida cruciale per la stabilità e la sicurezza geopolitica dell'Ue[60]. In una società iperconnessa ed interconnessa caratterizzata da forti legami transnazionali e interpretazioni pluraliste della democrazia è pertanto necessario e inevitabile un confronto più stretto tra i paesi membri.

La realizzazione di una visione unitaria a livello comunitario si scontra con criticità interne ai vari Stati, che ostacolano il raggiungimento di una posizione comune. Differenze di interessi, priorità e obiettivi specifici legati alla propria agenda politica, economica e sociale, inibiscono le esigenze di una gestione coordinata. Nel mentre, disparità economiche e di *status* sociale all'interno dei singoli Stati, che si manifestano anche nell'accesso alle tecnologie e alle competenze digitali, continuano a generare tensioni e conflitti che si ripercuotono sulla coesione sociale a vantaggio degli Stati e dei cittadini con maggiori risorse e competenze e a discapito di una visione di insieme. L'assenza di allineamento strategico si riflette inevitabilmente sulla capacità di definire standard, norme e regole condivise per una sovranità digitale che sembra diventare una vera e propria sfida.

Appare riduttivo affermare che la definizione delle modalità di trattamento e delle condizioni per il trasferimento transnazionale dei dati

55. Beck 2013.

56. L'*European Council on Foreign Relations* (ECFR) propone in un paper un nuovo concetto di Sovranità digitale intesa come la capacità di un Paese di governare le nuove tecnologie digitali e il loro impatto sulla società. L'organizzazione ne sottolinea la rilevanza, soprattutto dopo la pandemia di COVID-19, che ha dimostrato l'importanza fondamentale del digitale e dei dati per determinare il proprio destino, sia a livello personale che nazionale, in termini di resilienza economica e sanitaria. Inoltre, la crisi attuale spinge l'Europa a utilizzare in modo decisivo i dati come leva per rinnovare il proprio sistema produttivo e stimolare la ripresa economica. Si veda: *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*.

57. Si veda a tal proposito Mezzanotte 2022, in cui si evidenziano i pericoli della sovranità digitale di un Paese messa a rischio dagli attacchi hacker, che tendono ad intensificarsi durante i periodi di conflitto anche attraverso la diffusione di fake news e la creazione di deepfake. Sull'argomento si veda inoltre Bertoni 2019, p. 11. Sull'argomento si veda ancora di Pietropaoli 2019, in cui l'autore evidenzia come il concetto di cyberspazio sia destinato a cambiare la natura dei conflitti e quali danni sia possibile infliggere con un atto di guerra cibernetica. Ancora Pietropaoli 2023.

58. Pohle–Thiel 2020.

59. Si veda a tal proposito Ferrarese 2017. L'autrice sostiene che "Lo stato, inteso tipicamente come un soggetto unitario, quale era nella rappresentazione sovrana, nei vari regimi internazionali si rifrange in figure composite, come in un quadro cubista, dando luogo ad una situazione di prevalente "frammentazione" nello scenario internazionale, che riguarda sia le norme che l'autorità", facendo riferimento a Broude 2008.

60. Si veda a tal proposito Alù 2022, p. 253 in cui l'autore scrive che l'Europa aspira a conquistare la c.d. sovranità digitale, come obiettivo strategico di integrazione sovranazionale volto a realizzare un indispensabile riposizionamento geopolitico della propria centralità nella ridefinizione dei rapporti di forza esistenti su scala globale rispetto alle dinamiche conflittuali della predominante competizione tecnologica dualistica USA-Cina.

personali rappresentano l'espressione dell'esercizio di poteri sovrani da parte di uno Stato di diritto[61] quando sono ancora molte le criticità riscontrabili nel caso in cui i dati vengono raccolti in un Paese e trattati in uno ospitante[62]. Quest'ultimo potrebbe, difatti, imporre le sue regolamentazioni, causando potenziali conflitti normativi a danno dei cittadini[63].

Parimenti, non è sufficiente limitare il potere pervasivo e intrusivo delle grandi multinazionali senza prevedere forme di contrasto al sovranismo digitale[64] e all'esercizio del suo potere di controllo[65] attraverso i dati degli individui che tradotti in profili, identificati tramite flussi di dati, degradano, citando Deleuze, a soggetti "dividuali"[66].

Se «un cellulare è un congegno di rintracciamento che fa anche telefonate»[67], è innegabile che siano le *élite* economiche, tecnologiche e politiche a gestirne il controllo.

Un controllo tecno-sociale fondato sulla gestione degli algoritmi che sono gli elementi operativi dei dispositivi e basato sull'elaborazione dei dati degli algoritmi stessi che permette anche di prevedere comportamenti futuri grazie a modelli predittivi avanzati che consentono di classificare e profilare la vita degli individui[68] spingendoli nel cosiddetto "capitalismo della sorveglianza"[69].

Nessuna "microfisica" del potere, per riprendere Michel Foucault[70], potrebbe oggi prescindere dall'analisi dell'impatto dirompente del digitale sul nostro vivere, in privato e in pubblico, e sulla stessa dinamica democratica[71].

Per frenare l'estensione del Panopticon digitale[72], in cui la sorveglianza si fonde con il desiderio

61. Zeno-Zencovich 2016.

62. Si veda a tal proposito il Provvedimento n. 112 del 30 marzo 2023 del Garante Privacy con cui l'Autorità ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI società che gestisce la piattaforma di intelligenza artificiale ChatGPT per violazione delle norme a tutela della privacy. Si veda ancora il successivo comunicato stampa del 29 gennaio 2024 con cui il Garante notifica a OpenAI , l'atto di contestazione per aver violato la normativa in materia di protezione dei dati personali.

63. Mangiameli 2023; Bertola 2022.

64. Si veda a tal proposito Alpini 2022. L'autrice cita l'esempio del d.l. n. 105 del 2019 e succ.ve modifiche, intitolato "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" incentrato proprio sul concetto di sovranità nazionale e per questo criticato da una parte della dottrina quale espressione di sovranismo.

65. Si veda a tal proposito Frosini 1968; Rodotà 1973. Mantelero 2012, p. 135 ss.

66. Si veda a tal proposito Santaniello 2022 in cui l'autore cita la Dichiarazione italiana dei diritti in Internet fortemente voluta da Stefano Rodotà e la recente *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* elaborata dalla Commissione europea e da quest'ultima inviata al Parlamento europeo e al Consiglio il 26 gennaio 2022 per una sottoscrizione congiunta. Cita ancora la *Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori* e la *Dichiarazione di Lisbona – Democrazia digitale con uno scopo* in cui si evidenzia la necessità di incanalare la trasformazione digitale nel solco dei valori della *good governance* europea.

67. Assange 2013.

68. Strikwerda 2023.

69. Resta 2019, p. 199 ss. Sul punto, cfr. Simoncini 2019. Si veda Talia 2023, p. 517 in cui l'autore scrive che «il codice degli algoritmi di machine learning sta diventando sempre più il soggetto che stabilisce i termini in base ai quali viene vissuta la vita delle persone, non soltanto nello spazio digitale, ma anche nello spazio fisico della loro vita, eliminando così anche le ultime barriere che tra questi due spazi esistono e che sono destinate a essere abbattute del tutto».

70. Foucault 1982.

71. Farinosi 2011, pp. 180-189.

72. Il concetto di controllo è centrale nell'analisi del Panopticon, un'innovativa struttura carceraria concepita da Jeremy Bentham. Questo edificio, grazie alla sua peculiare architettura circolare che ruota attorno a una torre centrale, permette a un singolo sorvegliante di monitorare una moltitudine di detenuti. L'ingegno dell'architettura risiede nel fatto che i prigionieri, isolati in celle equidistanti, non possono vedere il sorvegliante, ma sono

di visibilità, creando un ciclo ininterrotto di controllo e auto-disciplina[73], è dunque necessario legare il concetto di sovranità (digitale) alla capacità di difendere i valori liberali e democratici.

Solo attraverso il rispetto dei principi e dei valori cardine posti a garanzia dei diritti fondamentali è difatti possibile scongiurare la pervasività del controllo e la manipolazione dei flussi informativi. Porre un freno alla violazione della privacy e così alle limitazioni delle libertà[74] è l'unico antidoto contro pericolose derive autoritarie. Questo presuppone un processo politico-culturale[75] che inizi a guardare con favore alla costruzione di un democratico concetto di sovranità digitale in cui riconoscere il rispetto della gerarchia delle fonti di diritto internazionale[76] e l'esistenza di un costituzionalismo digitale[77] demandato a codificare i diritti digitali[78] rappresenta il primo passo per

costantemente indotti a credere di essere osservati. Tale percezione perpetua di sorveglianza invisibile induce nei detenuti un comportamento conforme, favorendo la loro riabilitazione attraverso l'interiorizzazione della disciplina. Michel Foucault ha ripreso e ampliato questa riflessione, applicando il principio del Panopticon a diverse istituzioni totali come il carcere, i manicomi, le fabbriche, le scuole, la famiglia. Nella sua opera *Sorvegliare e punire*, Foucault argomenta che i meccanismi di controllo e sorveglianza, seppur sottili e spesso impercettibili, permeano la società contemporanea, creando una standardizzazione comportamentale. La società, inconsapevolmente sorvegliata, è modellata da un sistema di premi e punizioni volto a promuovere un'omogeneità di pensiero e azione, facilitando il controllo sociale. Con l'avvento dell'era digitale, il Panopticon si è trasformato in un nuovo paradigma di sorveglianza virtuale in cui la distinzione tra sorvegliante e sorvegliato si dissolve: ciascuno è contemporaneamente osservatore e osservato. La condivisione incessante di esperienze, preferenze e dettagli personali costruisce una narrazione pubblica della nostra identità, esponendola a un pubblico potenzialmente illimitato. Questo nuovo modello di controllo digitale è caratterizzato dalla raccolta e analisi di dati personali da parte delle grandi piattaforme, che li utilizzano per profilazione e pubblicità mirata a discapito della privacy. Così, il Panopticon virtuale di Bentham si realizza nella Rete, dove la sorveglianza si fonde con il desiderio di visibilità, creando un ciclo ininterrotto di controllo e auto-disciplina. Si veda a tal proposito Foucault 1976, pp. 21-22; Stanzione 2020.

73. Talia 2023.

74. Califano 2016; si veda ancora Colapietro 2018, p. 34, secondo cui la privacy «assume il carattere di "garanzia presupposto" dell'esercizio di altri diritti fondamentali, al fine di rendere possibile lo sviluppo della persona, l'esplicazione reale ed effettiva delle sue libertà».

75. Santaniello 2021, p. 595.

76. In particolare, quelle di protezione generale dei diritti umani come la *Dichiarazione Universale dei Diritti Umani* approvata dall'Assemblea delle Nazioni Unite a Parigi il 10 dicembre 1948, la *Convenzione Unesco*, firmata a Londra nel 1945, la *Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, firmata a Roma il 4 novembre 1950

77. Pollicino 2023.

78. Si veda a tal proposito Resta 2019, p. 222 in cui l'autore menziona il diritto a non essere oggetto di decisioni automatizzate; Jørgensen 2019; Cath 2018. Nel panorama nazionale Stefano Rodotà, in occasione del III Internet Governance Forum, avanzò una proposta di modifica costituzionale formulando un articolo 21-*bis* in base al quale «Tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale». L'art. 21-*bis*, tuttavia, non è stato assunto come dettame costituzionale ma la proposta di Rodotà, nel luglio 2015, è confluita nella *Dichiarazione dei diritti di Internet*, che riconosce come Internet abbia «contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Internet ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera». Internet, secondo questa linea di indirizzo, deve essere considerata come una risorsa globale che risponde al criterio della universalità e proprio per questo l'articolo 2 sancisce «l'accesso ad Internet come diritto fondamentale della persona e condizione per il suo pieno sviluppo

democratizzare la sovranità digitale e spingere gli individui ad autodeterminarsi[79] e ad esercitare il diritto di controllo sui propri dati [80].

Creare dunque un nuovo spazio di esercizio della sovranità, che trascende i confini geografici e si estende all'ambito digitale, permettendo ai cittadini di esercitare il loro potere e di partecipare attivamente alla vita politica in modo più efficace e inclusivo[81]. Rievocando l'idea di Rousseau, in una moderna democrazia, la sovranità appartiene al popolo e non ad un monarca[82]. In tal senso anche la sovranità digitale non può che elevarsi a spazio di esercizio e di azione della sovranità del popolo cui è demandata l'autorità di esercizio[83] dei propri diritti e interessi personali.

## 5. Conclusioni

La cybersecurity non può esaurirsi a un mero apparato tecnico normativo, ma deve elevarsi a baluardo della sovranità digitale, intesa non come sterile rivendicazione di potere, bensì come presidio dei diritti e delle libertà dei cittadini nel perimetro del *cyberspazio*. I due concetti trovano la loro più autentica espressione in una visione d'insieme che li colloca in una relazione di reciproca implicazione. Solo attraverso tale sinergia, ove sicurezza e sovranità si compenetrano in un nesso inscindibile, è dato ipotizzare un *corpus* normativo unitario che sorregga e informi l'azione statuale sulla base dei condivisi principi democratici.

La cybersecurity diviene condizione di possibilità per l'esercizio di una sovranità che, lungi dal rimanere ancorata a confini geografici, si proietta nella dimensione digitale, rendendosi garante dell'autodeterminazione informativa dei singoli e della comunità. Contestualmente, la sovranità digitale, non risolvibile in un mero atto di forza, trova la sua legittimazione ultima nella capacità di assicurare la sicurezza dei dati e delle informazioni, sottraendoli a ingerenze indebite e a utilizzi distorsivi. Due concetti fondamentali, per concludere, da intendersi come espressione di una volontà politica che si fa interprete di istanze di tutela e di promozione della persona umana, anche e soprattutto nel suo rapporto con le nuove tecnologie. L'auspicio è che si possa giungere a un cambio epocale di paradigma sulla base di un approccio radicale e innovativo in cui cybersecurity e sovranità digitale, cariche di una valenza etica, si pongano a tutela di una democrazia non ancorata a schemi obsoleti delineando il passaggio dall'*Internet of thing* al *Right over thing*.

## Riferimenti bibliografici

M.R. Allegri (2021), *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in "Rivista italiana di informatica e diritto", 2021, n. 2

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

A. Alù (2022), *La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A.C. Amato Mangiameli, M.N. Campagnoli (2020), *Strategie digitali. #diritto_educazione_tecnologia*, Giappichelli, 2020

individuale e sociale». L'articolo continua prevedendo che «Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale» Sull'argomento si veda Spagnuolo–Sorrentino 2021, pp. 276-286.

79. Mangiameli 2011.

80. Il rispetto dei principi di trasparenza, di non esclusività della decisione automatizzata e del consenso, sanciti dagli artt. 12, 13, 14, 15 e 22 del GDPR rappresentano il presupposto giuridico del controllo sui propri dati.

81. Si veda a tal proposito Santaniello 2022.

82. Noone 1970, pp. 696-708.

83. Couture–Toupin 2019; Pohle–Thiel 2020.

J. Assange (2013), *Internet è il nemico. Conversazione con Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann*, Feltrinelli, 2013

S. Autolitano, A. Pawlowska (2021), *Europe's Quest for Digital Sovereignty: Gaia X as a Case Study*, IAI Papers, 2021, n. 14

J.P. Barlow (1996), *Dichiarazione di indipendenza del Cyberspazio*, 1996

U. Beck (2013), *La società del rischio. Verso una seconda modernità*, Carocci, 2013

V. Bertola (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", fascicolo monografico a cura di L. Abba, A. Lazzaroni, M. Pietrangelo, 2022, n. 1

F. Bertoni (2019), *Deepfake, ovvero* Manipola et impera. *Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in "Ciberspazio e diritto", 2019, n. 1-2

B. Brighi, P.G. Chiara (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in "federalismi.it", 2021, n. 21

T. Broude (2008), *Fragmentation(s) of International Law: On Normative Integration as Authority Allocation*, in T. Broude, Y. Shany (eds.), "The Shifting Allocation of Authority in International Law: Considering Sovereignty, Supremacy, and Subsidiarity", Hart Publishing, 2008

L. Califano (2016), *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, 2016

A. Cassese (2006), *Diritto internazionale*, a cura di P. Gaeta, il Mulino, 2006

C. Cath (2018), *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*, in "Philosophical Transactions of the Royal Society A", 2018

F.Y. Chee (2024), *EU drops sovereignty requirements in cybersecurity certification scheme, document shows*, Reuters, 2024.

C. Colapietro (2018), *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Editoriale Scientifica, 2018

Commissione europea (2020), *Plasmare il futuro digitale dell'Europa*, 2020

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

M. Cuniberti (a cura di) (2008), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, 2008

J.-P. Darnis (2021), *L'Unione europea tra autonomia strategica e sovranità tecnologica: problemi e opportunità*, IAI Papers, 2021, n. 19

P. De Rosa (2021), *Concetto di Stato e nuove tecnologie. Quale ruolo per lo Stato nello spazio digitale?*, in "Media Laws", 2021, n. 1

Enisa - European Union Agency for Network and Information Security (2019), *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2019

Enisa - European Union Agency for Network and Information Security (2017), *Cyber Security Culture in organisations*, 2017

Enisa - European Union Agency for Network and Information Security (2016), *Definition of Cybersecurity: Gaps and overlaps in standardization*, 2016

M.S. Esposito (2019), *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in "Il Diritto dell'Informazione e dell'Informatica", 2019, n. 4-5

M. Farinosi (2011), *Beyond the panopticon framework: Privacy, control and user generated content*, in A. Esposito, A.M. Esposito, R. Martone et al. (eds.), "Toward Autonomous, Adaptive, and Context-Aware Multimodal Interfaces. Theoretical and Practical Issues", Springer, 2011

M.R. Ferrarese (2017), *Il diritto internazionale come scenario di ridefinizione della sovranità degli Stati*, in "Stato e mercato", 2017, n. 109

F. Faini (2019), *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 4-5

F. Faini (2019-a), *Diritto all'esistenza digitale*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 3

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

G. Finocchiaro (2014), *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro, F. Delfini (a cura di), "Diritto dell'informatica", UTET, 2014

R. Flor (2019), *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in "Diritto di internet", 2019, n. 3

L. Floridi (2015), *The Onlife Manifesto*, Springer, 2015

L. Floridi (2009), *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli, 2009

C. Formenti (2008), *Cybersoviet. Utopie postdemocratiche e nuovi media*, Raffaello Cortina Editore, 2008

M. Foucault (1982), *Microfisica del potere: interventi politici*, vol. 90, Einaudi, 1982

M. Foucault (1976), *Sorvegliare e punire. Nascita della prigione*, Einaudi, 1976

P.W. Franzese (2009), *Sovereignty in Cyberspace: Can It Exist?*, in "The Air Force Law Review", vol. 64, 2009

V. Frosini (1968), *Cibernetica, diritto e società*, Edizioni di Comunità, 1968

D.-U. Galetta (2018), *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, in "Ciberspazio e diritto", 2018, n. 3

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

D. Harvey (2006), *La guerra perpetua. Analisi del nuovo imperialismo*, Il Saggiatore, 2006

P. Hummel, M. Braun, M. Tretter, P. Dabrock (2021), *Data sovereignty: A review*, in "Big Data & Society", vol. 8, 2021, n. 1

R.F. Jørgensen (ed.) (2019), *Human Rights in the Age of Platforms*, MIT Press, 2019

T. Madiega (2020), *Digital Sovereignty for Europe*, European Parliamentary Research Service, PE 651.992, July 2020

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

S. Mangiameli (2023-a), *La sovranità digitale*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023

S. Mangiameli (2011), *Autodeterminazione: diritto di spessore costituzionale?*, in C. Navarini (a cura di), "Autonomia e autodeterminazione. Profili etici, bioetici e giuridici", Editori Riuniti, 2011

A. Mantelero (2012), *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in "Il diritto dell'informazione e dell'informatica", 2012

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

M. Mezzanotte (2022), *Fake news, deepfake e sovranità digitale nei periodi bellici*, in "federalismi.it", 2022, n. 33

L. Moerel, P. Timmers (2021), *Reflections on Digital Sovereignty*, in "EU Cyber Direct, Research", Focus series, 2021

J.B. Noone (1970), *The Social Contract and the Idea of Sovereignty in Rousseau*, in "The Journal of Politics", vol. 32, 1970, n. 3

M. Orofino (2018), *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in "MediaLaws", 2018, n. 2

P. Passaglia (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei* social media*, tra regole generali e ricerca di una specificità*, in "ConsultaOnline", 2016, n. 3

S. Pietropaoli (2023), *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, in "Ars interpretandi", 2023, n. 1

S. Pietropaoli (2019), *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in "Rivista di filosofia del diritto", 2019, n. 2

F. Pizzetti (2016), *Privacy e il diritto europeo alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Giappichelli, 2016

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

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

O. Pollicino, E. Bertolini, V. Lubello (a cura di) (2013), *Internet: regole e tutela dei diritti fondamentali*, Aracne, 2013

G. Resta (2019), *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, n. 2

S. Rodotà (2006), *Tecnologie e diritti*, il Mulino, 2006

S. Rodotà (1973), *Elaboratori elettronici e controllo sociale*, il Mulino, 1973

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

M. Santaniello (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

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

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

A. Simoncini, E. Cremona (2022), *La AI fra pubblico e privato*, in "DPCE Online", 2022, n. 1

A.F. Spagnuolo, E. Sorrentino (2021), *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in "federalismi.it", 2021, n. 8

P. Stanzione (2020), Intervento al Security Summit 2020, sessione "La sovranità tecnologica e digitale dell'Unione Europea: il difficile ruolo di mediazione con gli over the top e i rapporti con gli USA", 12 novembre 2020

L. Strikwerda (2023), *Predictive identification als een moreel ondoor-zichtig panopticon*, in "PROCES", 2023, n. 3

D. Talia (2023), *Il potere disciplinare della governamentalità digitale*, in "Rivista di Digital Politics" 2023, n. 3

P.A. Walker (2015), *Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace*, in M. Maybaum, A.M. Osula, L. Lindstrom (eds.), "Architectures in Cyberspace", 7th International Conference on Cyber Conflict, 2015

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

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019