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

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0196 • articolo sottoposto a peer review • pubblicato in anteprima il 19 dic. 2024

Marina Pietrangelo

La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo

Il saggio esamina criticamente alcuni aspetti dell'attuale assetto di governo della cybersicurezza. Muovendo da una ridefinizione estensiva del concetto, si prospettano una maggiore valorizzazione degli interventi di carattere sociale e un rafforzamento delle azioni istituzionali di controllo e collaborazione.

Profili giuridici della cybersicurezza – Governo della cybersicurezza – Governance digitale
Dimensione sociale della cybersicurezza

The plural dimension of cybersecurity: from invisible power to collaborative process

The paper critically examines some aspects of the current cybersecurity's legal framework. The concept of cybersecurity is extensively redefined to highlight some critical issues. The main demand is for social measures and forms of institutional control and cooperation.

Legal aspects of cybersecurity – Cybersecurity government – Digital governance – Cybersecurity awareness

L'Autrice è prima ricercatrice presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

1. Premessa. La cybersicurezza come "condizione di esistenza" della digitalizzazione

Negli ultimi decenni la governance del digitale ha polarizzato il dibattito pubblico e la riflessione scientifica. Sono stati censiti e analizzati diversi modelli di gestione e governo dello spazio digitale; e ne sono stati proposti di nuovi, spesso con l'obiettivo di appianare o risolvere sbilanciamenti e contrasti già consolidati tra poteri pubblici e poteri privati[1]. La digitalizzazione pervasiva e totalizzante, benché ancora "in transito", ha infatti travolto e mutato non soltanto gli stili di vita delle persone nella loro quotidianità professionale e di relazione, ma anche gli apparati delle istituzioni e la declaratoria delle relative loro funzioni[2]. Nuove autorità con nuovi poteri richiesti dalla mole di incombenze connesse agli usi delle tecnologie digitali sono subentrate nella mappa di poteri preesistente, affiancandoli, talvolta sovrapponendosi ad essi, tal altra guadagnando in modo non sempre trasparente porzioni rilevanti di capacità decisionale. L'esigenza di fare presto per supportare la decisiva transizione digitale e assicurare alla collettività un'adeguata protezione dagli abusi di cui i processi di digitalizzazione pure sono costellati ha di fatto finito per esautorare le sedi della rappresentanza e del controllo, in favore di una supposta maggiore efficienza della decisione governativa: un modello verticale di esercizio del potere pubblico digitale, che tradisce però l'idea di una sovranità digitale tutta imperniata sulle misure tecniche di cybersicurezza e scollegata dalla sua dimensione sociale.

1. Per uno sguardo d'insieme, v. Bradford 2023, che mette bene a fuoco i tre diversi modelli di governo del digitale (Usa, Cina e Ue) e Soro 2019; Finocchiario–Balestra–Timoteo 2022; e volendo, Abba–Lazzaroni –Pietrangelo 2022. Sul "rapporto tra poteri", v. in particolare Torchia 2024; Pollicino 2023, pp. 410 ss.; Resta 2023, p. 1008 ss.; Ferrarese 2022; Betzu 2021. Sulle evoluzioni delle categorie oggettive e soggettive del diritto contemporaneo, non soltanto in relazione ai poteri e al governo dello spazio digitale, v. ampiamente Zaccaria 2022, che individua nella coppia "destrutturazione-pluralismo" la chiave di lettura delle modificazioni dell'ordine giuridico contemporaneo. La prima formula indicherebbe l'insieme di fattori di crisi e di alterazione dell'assetto giuridico tradizionale, i cui soggetti, strumenti ed enti «sono costretti a continuare le loro funzioni pur in un quadro ampiamente e strutturalmente mutato» (p. 13). Il secondo termine della coppia vorrebbe rappresentare l'apertura pluralistica «alla presenza e all'azione di un maggior numero di soggetti, pubblici e privati» (*ivi*).
2. Così Ferrarese 2022, *passim*, la quale analizza due distinti fenomeni di mutamento del quadro dei poteri negli ultimi anni del Novecento significativamente condizionati dallo sviluppo tecnologico: il "trasloco" del potere, che non abita più «necessariamente solo in palazzi governativi e statali, con note etichette ufficiali, ma ha trovato nuove residenze sia in sedi internazionali, sia specialmente in sedi private, smettendo di indossare i consueti abiti istituzionali sotto l'egida del diritto pubblico» (p. 9); e la sua "metamorfosi", cioè un mutamento nel «modo di essere e di presentarsi» (*ibidem*), che è ravvisabile nella «diffusa tendenza a ri-forgiare le modalità e le forme di potere, producendo misture, travasi e confluenze di vario tipo, nonché creando nuovi canali di scorrimento spesso di tipo orizzontale» (*ibidem*). Sul punto, v. anche Zaccaria 2022, specie p. 37 ss.

Si tratta di modificazioni "strutturali" del nostro ordinamento costituzionale che paiono andar ben al di là di quanto previsto dal dettato normativo, aprendo nuovi fronti in una crisi istituzionale ancora irrisolta, per molta parte occasionata proprio dall'erompere di nuovi "poteri tecnologici"[3].

Occorre allora interrogarsi sugli effetti, oltre che sulle intuibili ragioni, di questo disegno istituzionale, alla ricerca di correttivi e interventi capaci di riportare l'esercizio del potere pubblico nell'alveo di un sistema rappresentativo nel quale le misure di controllo e partecipazione recuperino il legittimo spazio sul protagonismo assoluto degli apparati governativi. Ciò anche in ragione della continua erosione del circuito della rappresentanza, già di per sé svilito da una produzione normativa frammentata e mossa da contingenze o stati emergenziali (oggettivi o dichiarati)[4].

Parallelamente, occorre coltivare un approccio estensivo alla cybersicurezza, che ne valorizzi in modo permanente la dimensione sociale – e dunque le misure di carattere educativo-formativo, sociale e sanitario – tutte decisive per elevare il grado complessivo di sicurezza del Paese (cosiddetta *cyber security awareness*)[5]. Agendo su entrambi i fronti, cioè maggiore controllo sugli apparati governativi e rafforzamento della collaborazione tra enti per attivare misure sociali diffuse, si conterrebbe l'espansione senza contrappesi di un nuovo potere, che sembra farsi sempre più assoluto e invisibile[6].

2. Il modello politico-amministrativo nazionale di cybersicurezza: coordinamento o accentramento

La definizione normativa che ricorre nella fitta e stratificata regolazione in materia, funzionale anzitutto all'applicazione di obblighi di adeguamento o ripristino delle misure minime di sicurezza informatica, pure se necessaria, risulta oggi riduttiva sotto il profilo concettuale[7]. Essa, infatti, riconduce la cybersicurezza nell'alveo primigenio della

3. Ben evidenzia le molte questioni poste dall'erompere del potere tecnologico nell'ordinamento costituzionale Simoncini 2022, pp. 133-154, il quale ritiene che vadano indagate con un nuovo approccio «"ibrido", capace cioè di utilizzare diverse forme di propulsione, così come un linguaggio e un metodo di analisi comprensibili sia dal regolatore che dal regolato» (p. 147). E al riguardo, a proposito della regolazione delle applicazioni di intelligenza artificiale, suggerisce due vie da esplorare, attingendo al diritto privato della concorrenza e al diritto amministrativo. Per il caso specifico della cybersicurezza, v. Vedder 2019, p. 11 ss.
4. Sul punto, v. le considerazioni recenti di Staiano 2024.
5. V. al proposito il rilievo assegnato dal National Cyber Security Center dell'UK alla "cyber hygiene" e alle azioni collettive: «(…) Defending the UK's democratic institutions and processes is a priority for the NCSC. However, it is not something we can achieve alone. It requires a collective effort across the whole of society, including industry and in partnership with allies, to defend our values and make the UK an unattractive environment for hostile actors. Our democracy is founded on the principle of participation; every member of the public across the four nations of the UK has a stake, and everyone has a role to play in defending it.» (*NCSC Annual Review* 2023, p. 41). Il tema della consapevolezza è oggi sempre più decisivo, visto anche l'aumento negli ultimi mesi di attacchi sofisticati che riescono ad aprire una backdoor sui sistemi delle vittime senza bisogno di alcuna interazione. Mediante la tecnica del *drive-by-compromise* l'utente-vittima naviga su un browser vulnerabile che lo indirizza su un sito fake, cioè su un social engineering che ridistribuisce URL malevoli. Cfr. il caso recente dei RomCom RAT, su cui Lakshmanan 2024. Sull'approccio "olistico" alla cybersicurezza, v. ampiamente le attività del progetto PNRR SERICS (*Security and Rights in CyberSpace*), finanziato dall'Unione europea nel programma NextGenerationEU, cui sono in parte riconducibili le riflessioni sviluppate in questa Sezione monografica.
6. Sulla rilevanza della collaborazione, v. ampiamente Baldoni 2024.
7. Secondo la definizione del DPCM 17 febbraio 2017 la cybersicurezza è l'insieme di «idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebito di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi». Con la direttiva UE 2022/2555, 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

normazione tecnica settoriale, entro cui sono nate e sono state elaborate le prime definizioni di cybersecurity, computer security e information security[8]. Con la massiva penetrazione sociale delle applicazioni digitali, la sicurezza informatica intesa come sicurezza di sistemi, reti e dati a fini di protezione da abusi e manomissioni ha registrato tuttavia una vera e propria estensione semantica, in ragione della quale essa è oggi ricondotta alle attività di sicurezza pubblica preordinate alla protezione degli interessi nazionali, alla stabilità delle istituzioni e all'ordinato vivere civile[9]. Per conseguenza, l'attribuzione di compiti e funzioni in materia di cybersicurezza ha coinciso con la relativa declaratoria costituzionale e normativa. Nel contesto geopolitico e socio-economico attuale sta invero emergendo e consolidandosi una ulteriore evoluzione del concetto, in cui al profilo già consolidato della sicurezza (informatica) pubblica come insieme di misure di protezione dell'interesse nazionale si sono addentellati nuovi ambiti connessi e interrelati, per nulla secondari, che anzi irrobustiscono la cybersicurezza come processo, chiamando in causa con sempre maggiore urgenza altri attori istituzionali. Si pensi alla sfera della organizzazione e gestione autonoma dei patrimoni informativi pubblici o ai servizi pubblici online erogati dagli enti territoriali: tutti beni o servizi digitali dei quali occorre garantire la sicurezza, assicurandone la continuità, col fine ultimo di tutelare i diritti degli "utenti"[10]. In uno scenario socio-economico sempre più complesso, non pare per esempio sufficientemente esplorata l'opportunità di «sistematizzare un canale di comunicazione/collaborazione stabile tra il livello nazionale e quello regionale/locale, affinché i territori interessati vengano prontamente allertati»[11] o di coinvolgere stabilmente i diversi livelli di Governo, attraverso il sistema delle conferenze o mediante la costituzione di una specifica nuova sede istituzionale. Un coinvolgimento diretto che favorirebbe peraltro la condivisione di processi già avviati o consolidati (si pensi per esempio ai percorsi di *Security Awareness Training*) e di non ripetere gli errori del passato in tema di digitalizzazione, evitando cioè approdi disomogenei e non condivisi. Come noto, uno dei fattori di maggior successo degli attacchi informatici rivolti ai sistemi delle amministrazioni pubbliche locali è proprio la tardiva digitalizzazione, spesso non corredata di adeguate misure formative.

Se dunque gli attacchi informatici sono una "questione di interesse pubblico"[12], l'interesse

direttiva (UE) 2016/1148 (cosiddetta NIS 2, recepita in Italia col d.lgs. 4 settembre 2024, n. 138), le misure di gestione dei rischi devono ora comprendere azioni tecniche, ma anche operative e organizzative (cfr. l'art. 21 della direttiva), secondo un approccio cosiddetto "multirischio".

8. Così Rizzi–Serini 2024, specie p. 7 ss., cui si rinvia per una più ampia ricostruzione del percorso di transito e ingresso – dalla normazione tecnica agli ordinamenti giuridici – dei concetti su richiamati.
9. Corte costituzionale 14 giugno 1956, n. 2: «Esclusa l'interpretazione, inammissibilmente angusta, che la "sicurezza" riguardi solo l'incolumità fisica, sembra razionale e conforme allo spirito della Costituzione dare alla parola "sicurezza" il significato di situazione nella quale sia assicurato ai cittadini, per quanto è possibile, il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'"ordinato vivere civile", che è indubbiamente la meta di uno Stato di diritto, libero e democratico.» (Diritto, n. 5). Sulla dimensione giuridica della sicurezza pubblica, v. ampiamente Mosca 2021; Ursi 2022; Ursi 2023.
10. Cfr. sul punto Conferenza unificata 8 luglio 2021 (rep. atti. n. 70), Parere, ai sensi dell'articolo 9 del decreto legislativo 28 agosto 1997, n. 281, sul decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionali.
11. *Ibidem*. Su questa linea v. la recente l.r. Regione Toscana 9 dicembre 2024, n. 57 recante *Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009*.
12. Cfr. il Considerando 1 del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), ove si legge «Gli attacchi informatici costituiscono una *questione di interesse pubblico* dal momento che hanno

pubblico alla cybersicurezza non può che essere interesse *della* e *per la* collettività, un obiettivo ambizioso perseguibile mediante azioni di cyberesilienza tecnico-economica accompagnate e mai disgiunte da misure preventive continue e capillari di cultura della sicurezza informatica[13]. Occorre cioè considerare come immanenti e necessarie – e non suppletive o di corredo – per la resilienza cybernetica le misure di carattere educativo-formativo e socio-sanitario: esse sole possono infatti elevare il grado di cybersicurezza del Paese in termini di consapevolezza a livello individuale o di ente. Una dimensione plurale della cybersicurezza cui deve corrispondere una molteplicità di azioni, funzionali a valorizzare sia la soluzione tecnica sia il fattore umano (e con esso il "fattore sociale")[14].

D'altro canto, proprio le modificazioni istituzionali occasionate dall'urgenza di governare e regolare le evoluzioni tecniche più di altre paiono scavare carsicamente nell'ordinamento costituito. Corrono cioè sottotraccia mutamenti che paiono andare ben al di là delle attribuzioni normative di nuove funzioni e nuovi compiti; e che richiamano alla mente il tema della visibilità del potere[15]. È grande cioè il sospetto che la cybersicurezza si identifichi oggi in un potere molto specializzato e poco visibile, malcelato sotto le vesti riabilitative di un decisore pubblico che suo tramite punta a recuperare la primazia nella complessa mappa dei poteri digitali[16]. Certo è che nelle politiche e pratiche della transizione digitale la cybersicurezza è oggettivamente una condizione di esistenza: rendere più sicuri reti, sistemi e dati vuole dire giocoforza rendere più sicuri gli Stati e i loro apparati, le persone e le loro vite. Una specie di protezione delle protezioni, una sicurezza maxima da cui dipendono le sorti delle Nazioni come degli individui, tutti inesorabilmente immersi nella dimensione digitale: la rilevanza democratica della gestione della cybersicurezza non pare dunque più in discussione[17]. Anzi, essa è oggi divenuta quasi uno strumento di "riscossa" degli Stati e del potere pubblico, che con essa tornano simbolicamente a farsi salvifici proprio a garanzia degli interessi della collettività che si muove nello spazio digitale[18].

---

un impatto determinante non solo sull'economia dell'Unione, ma anche *sulla democrazia*, nonché sulla sicurezza dei consumatori e sulla salute.» (corsivi aggiunti). Gli attacchi informatici aumentano costantemente. Secondo il Rapporto Clusit 2024, nel primo semestre 2024 gli attacchi sono «cresciuti del 23% rispetto al semestre precedente. In media, si sono verificati nel mondo 9 attacchi importanti al giorno; in Italia il 7,6% degli incidenti. La sanità è il settore più colpito a livello globale. In Italia bersagliato il manifatturiero, ma gli attacchi alla sanità crescono dell'83% rispetto al primo semestre 2023» (cfr. Clusit 2024, p. 7).

13. Distingue tra nozione estesa di cybersicurezza, che interessa il livello socio-cognitivo – cioè l'insieme delle relazioni umane –, e nozione ristretta, che invece riguarda la protezione dei livelli fisico-infrastrutturale e logico-informativo, Ursi 2023, pp. 7 ss.
14. V. ampiamente Clusit 2024.
15. Ferrarese 2022 si chiede se tali nuovi poteri siano ancora riconducibili alla «"tunica" larga e accogliente» (p. 48) di una governance in cui i poteri sono visibili, richiamando sul punto gli scritti di Norberto Bobbio sulla democrazia come governo del potere visibile.
16. Su tali profili v. Longo 2024.
17. Il tema è ben presente da almeno un ventennio negli indirizzi politici eurounionali. Cfr. già COM(2001) 298 *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, secondo cui «La sicurezza sta diventando un tema di assoluta priorità perché le comunicazioni e le informazioni sono ormai fattori determinanti dello sviluppo economico e sociale. Le reti e i sistemi di informazione veicolano un volume e una pluralità di servizi e dati ancora inconcepibili fino a pochi anni fa. La loro disponibilità è essenziale per altre infrastrutture quali la rete idrica e la rete elettrica. Poiché tutti, dall'impresa al cittadino privato, alla pubblica amministrazione, desiderano avvalersi delle possibilità offerte dalle reti di comunicazione, la sicurezza di tali sistemi diventa un presupposto essenziale per ulteriori progressi» (p. 6). La comunicazione già riconduceva le misure in materia di sicurezza informatica alle politiche in materia di telecomunicazioni, protezione dei dati e criminalità informatica.
18. In tal senso, ancora Ferrarese 2022, pp. 153 ss.

In questo scenario, tuttavia, l'ancoraggio esclusivo della cybersicurezza alle funzioni di protezione della sicurezza nazionale e la conseguente definizione a livello interno di un reticolo di funzioni e compiti tutti riferibili agli apparati di Governo tradiscono un approccio verticale e tecnicistico, che trascura la sua dimensione plurale[19].

D'altro canto, il quadro regolatorio eurounionale esclude un approdo di tipo securitario, cioè il rafforzamento della cybersicurezza imperniato soltanto su meccanismi reattivi (se non addirittura repressivi e sanzionatori), ma non preclude differenziazioni in fase di adeguamento. Per tale ragione è quantomai opportuna la ricerca di soluzioni regolatorie e attuative il più possibile distanti da modelli di tipo impositivo, rimessi cioè alla mera adozione di nuovi carichi regolatori (oneri e obblighi) specie su soggetti privati (piccole e medie imprese) e amministrazioni pubbliche. Tali considerazioni paiono più ancora necessarie ove si considerino taluni ulteriori profili della cybersicurezza, come la cyberdefence o la cyberintelligence, che spingono verso una sempre maggiore autonomia della funzione mantenendola evidentemente saldamente innestata nella sola azione di Governo[20], e talune nuove proposte regolatorie attualmente all'esame del Parlamento.

2.1. I settori interrelati con la funzione di cybersicurezza

Le nuove e più severe misure di cybersicurezza introdotte dalla normativa recente interessano i settori economici più diversi, da quello bancario e finanziario al settore dell'energia, dal settore alimentare a quello dei servizi digitali (infrastrutture, reti, e-commerce, motori di ricerca, cloud ecc.) oltre che le attività delle amministrazioni pubbliche[21]. L'obiettivo principe di tale regolazione resta quello di prevenire e gestire gli attacchi informatici, e su questo aspetto i dati del *Global Cybersecurity Index 2024* collocano l'Italia tra i Paesi più virtuosi[22]. Si tratta ovviamente di un monitoraggio orientato e condizionato da una visione tecnocentrica, ontologicamente espressa peraltro dall'ITU, la quale non considera altre rilevanti variabili, riferibili alla dimensione plurale di cui si è detto sopra. Manca per esempio una griglia delle competenze e degli interventi diffusi che per via mediata impattano significativamente sul livello complessivo di cybersicurezza[23]. Un esame più capillare dei dati relativi agli attacchi informatici andati a buon fine negli ultimi mesi, rivolti ai sistemi IT di amministrazioni pubbliche o imprese di piccole e medie dimensioni, mostra proprio una vulnerabilità complessiva ampia e sfaccettata, certamente di tipo tecnico-strutturale, ma non soltanto. L'efficacia degli

19. Sul rapporto tra tecnica e decisione politica, v. ampiamente Cardone 2021.
20. Sulla cybersicurezza come funzione amministrativa autonoma, v. le considerazioni di Ursi 2023. Sulla ulteriore vercalizzazione dei poteri di sicurezza pubblica v. il ddl AC1236 (Diposizioni in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario) di iniziativa del Ministro dell'interno (Governo Meloni-I) già approvato dalla Camera e alla data attuale in commissione in Senato.
21. Ultimo in ordine di tempo è il regolamento (UE) 2024/2847 già citato. Di recente recepimento sono poi le due direttive n. 2022/2555 sulla resilienza dei soggetti critici e n. 2022/2557 (cosiddetta NIS 2) recepite coi decreti legislativi nn. 134 e 138 del 2024. I due decreti sono stati approvati in via definitiva dal Consiglio dei Ministri nella seduta n. 91 del 7 agosto 2024, a seguito dell'esame parlamentare per i pareri concluso il 27 luglio (sull'iter dello schema di decreto legislativo, cfr. XIX leg., Camera dei deputati, Atto del Governo n. 164). Per uno sguardo di sintesi sulla regolazione in materia di cybersicurezza, v. Longo 2024-a, p. 203 ss. In particolare, sulla direttiva NIS 2, v. Casarosa–Comandè 2024; Buffa 2023; Bavetta 2022; Zorzi Giustiniani 2022, p. 56.
22. Cfr. ITU 2024. Il rapporto si basa sui dati forniti dai punti di contatto nazionali (in Italia l'ACN) ed è poi elaborato secondo un approccio multi-stakeholder. L'Italia rientra tra i Paesi più virtuosi assieme ad altri 45 Stati, ritenuti molto solidi in relazione ai cinque parametri usati per la classificazione (Legal, Technical, Organizational, Capacity Development, Cooperation Measures).
23. In tal senso, v. Clusit 2024, in particolare l'*Approfondimento Italia e PA*, che riferisce di un aumento esponenziale del numero di attacchi rivolti alle piccole e piccolissime pubbliche amministrazioni, probabilmente a causa dei ritardi nel percorso di digitalizzazione e formazione del personale in termini di cultura del digitale.

attacchi trova per esempio nel tardivo o parziale processo di digitalizzazione e nell'assenza o nell'inadeguatezza di percorsi formativi sulla sicurezza informatica e sulla gestione del rischio un grande alleato. Resta, dunque, centrale la dimensione ampia e poliedrica della cybersicurezza, per il cui rafforzamento sono determinanti l'azione socio-educativa sul territorio, il supporto amministrativo locale alle piccole e piccolissime imprese, le azioni di monitoraggio e partecipazione sui territori.

Se cioè la cybersicurezza deve essere un'agonista della transizione digitale, è bene che nella sua governance vengano innestati adeguati contrappesi e che si attivino altre competenze, nella misura in cui esse risultino tanto legittime quanto necessarie[24]. Si pensi per esempio ai settori liminari alla dimensione dell'"ordine pubblico e della sicurezza", cioè a quei settori confinanti con tale materia che spetta in via esclusiva al legislatore statale, ma che per l'appunto non esclude interventi regionali[25]. L'intervento dello Stato cioè in "materia" di sicurezza non escluderebbe interventi regionali in settori confinanti, meno a rischio di erosione rispetto ad esempio ai casi di materie trasversali come il coordinamento informatico che di fatto attraversano, attraendone parti, spazi limitrofi di competenza regionale[26]. Accanto alla "sicurezza in 'senso stretto' (o *sicurezza primaria*)"[27] che spetta allo Stato esistono ambiti di "sicurezza secondaria (o *sicurezza in senso lato*)"[28], che ricomprende «un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale»[29] e che risponde a quell'esigenza di coordinamento tra Stato e Regioni che la legge statale può disciplinare anche nella materia dell'ordine pubblico e sicurezza (*ex* art. 118, terzo comma, Cost.). Con riguardo all'ambito della digitalizzazione e alla sicurezza delle persone nello spazio digitale si può qui menzionare il caso del contrasto al cyberbullismo[30], che richiede interventi non soltanto di tipo penale o di polizia, ma anche e soprattutto di carattere educativo e social-preventivo[31]. Non sono neppure mancate talune sperimentazioni linguistico/normative, come quella

24. Evidenzia i limiti delle attuali forme di controllo parlamentare sulle attività di cybersicurezza facenti capo alla Presidenza del Consiglio e all'Agenzia per la Cybersicurezza Giupponi 2024, specie p. 297. Più in generale, con uno sguardo filosofico e pragmatico assieme, sui modelli di governance del digitale, interessanti le osservazioni di Benanti 2022, specie le pp. 133 ss., che prospetta una governance delle intelligenze artificiali inclusiva, in cui si annodano aspetti tecnici ed etici, la quale dovrebbe intercettare tutta la comunità di riferimento per definire assetti organizzativi e regole possibili (i migliori possibili).
25. Corte cost. sentenza n. 226 del 2010, Diritto 5.2, che richiama *ex plurimis* le sentenze n. 129 del 2009; n. 237 e n. 222 del 2006; n. 383 e n. 95 del 2005; n. 428 del 2004.
26. Cfr. Corte cost. n. 285 del 2019, Diritto 2.3, in cui si legge «Per costante orientamento di questa Corte, allora, l'endiadi "ordine pubblico e sicurezza", di cui all'art. 117, secondo comma, lettera h), Cost., allude a una materia in senso proprio, e cioè a una materia oggettivamente delimitata che di per sé non esclude l'intervento regionale in settori ad essa liminari».
27. *Ibidem*.
28. *Ibidem*.
29. *Ibidem*.
30. In tal senso, v. la l.r. Regione Umbria 9 maggio 2018, n. 4 (*Disciplina degli interventi regionali per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo – Modificazioni a leggi regionali*), che ha superato il vaglio della Corte Costituzionale, secondo cui la Regione si è legittimamente mossa nell'ambito della propria competenza di promozione culturale e politica socio-assistenziale, senza "tracimare" in quella statale della tutela dell'ordine pubblico e della sicurezza: «Il legislatore regionale è piuttosto intervenuto in un'ottica di prevenzione del bullismo quale problema di interesse sociale generale, per tutelare e valorizzare la crescita educativa, sociale e psicologica dei minorenni, perseguendo finalità di prevenzione, estranee alla materia della tutela dell'ordine pubblico e della sicurezza.» (Corte cost. n. 116 del 2019, Diritto 3.4.)
31. Sul modello securitario nell'approccio del legislatore statale, v. ampiamente le riflessioni a prima lettura sulla legge n. 90/2024 contenute nei saggi apparsi in Fiorinelli–Giannelli 2024.

relativa al "sistema integrato e unitario di sicurezza nazionale"[32], che vuole alludere alla pluralità degli interventi di soggetti diversi ciascuno nell'ambito delle proprie competenze e responsabilità. Si tratta di un terreno già arato, nel solco del quale potrebbe avviarsi forse una riflessione anche per i profili di nostro interesse. Per quanto, anche tale modello – come evidenziato nella letteratura più avveduta sulla materia – parrebbe confermare un'impronta securitaria di tipo verticale[33].

Nel quadro sopra delineato, si consideri poi che per numerosità e ampiezza di compiti un ruolo di assoluto protagonismo spetta all'Agenzia per la Cybersicurezza Nazionale (ACN). Pur se di recente istituzione (2021), molte e approfondite risultano già le riflessioni sulla sua natura giuridica, e specialmente su compiti e funzioni ad essa assegnati[34]. Senza qui entrare nel dettaglio di un reticolo regolativo che s'infittisce al pari dell'aumento delle minacce cyber, occorre qui almeno segnalare che parimenti cresce il numero di compiti affidati alla nostra agenzia[35].

In tale direzione vanno per esempio le proposte contenute nel disegno di legge d'iniziativa governativa AS1146 in materia di intelligenza artificiale, attualmente all'esame del Senato come collegato alla legge di bilancio[36].

Tale progetto, infatti, assegna all'ACN ulteriori nuovi compiti, tra cui quello di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, finalizzata a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, concentrando in essa poteri che pure potevano convergere su altre autorità[37]. Se il disegno di legge verrà adottato nel testo attualmente in discussione, dunque, all'ACN,

32. La formula è tratta dall'art. 1, co. 2, del d.l. 20 febbraio 2017, n. 14 (*Disposizioni urgenti in materia di sicurezza delle città*), conv. con modifiche nella legge n. 48/2017: «Ai fini del presente decreto, si intende per sicurezza integrata l'insieme degli interventi assicurati dallo Stato, dalle Regioni, dalle Province autonome di Trento e Bolzano e dagli enti locali, nonché da altri soggetti istituzionali, al fine di concorrere, ciascuno nell'ambito delle proprie competenze e responsabilità, alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali.» Il "benessere delle comunità territoriali" giustificherebbe quindi la previsione legislativa di forme di coordinamento tra Stato e Regioni, e la promozione della sicurezza integrata deve tener conto «(…) della necessità di migliorare la qualità della vita e del territorio e di favorire l'inclusione sociale e la riqualificazione socio-culturale delle aree interessate» (art. 2, co. 1-*bis*). Secondo Famiglietti 2020, si tratterebbe però di una definizione «più che volta a delimitare l'ambito contenutistico degli interventi, ad individuare i soggetti protagonisti della "sicurezza integrata" e gli strumenti volti al perseguimento degli obiettivi» (p. 177).
33. Sulla persistenza di una impronta verticale. v. Antonelli 2017; Nobili 2018, p. 61 ss.
34. Tra gli altri, v. Giupponi 2024; Ricotta 2023, p. 97 ss.; Golisano 2022; Forgione 2022; Sola 2022; Contaldo 2023; Poletti 2023; volendo, Pietrangelo 2024; Giannelli 2024.
35. Cfr. al proposito il DPCM 15 giugno 2022 e il DPCM 1° settembre 2022, mediante cui sono state trasferite in capo all'Agenzia per la Cybersicurezza Nazionale le funzioni in materia di cybersicurezza precedentemente assegnate al Ministero dello Sviluppo Economico (MISE), all'Agenzia per l'Italia digitale (AgID) e al Dipartimento per la trasformazione digitale della PCM.
36. XIX leg., AS 1146 (Disposizioni e delega al Governo in materia di intelligenza artificiale), d'iniziativa del Presidente del Consiglio e del Ministro della giustizia (Governo Meloni-I). Il ddl è attualmente all'esame in sede referente presso le Commissioni riunite 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10ª (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale).
37. Cfr. l'art. 16 del ddl, che modifica l'art. 7, comma 1, del d.l. 14 giugno 2021, n. 82 istitutivo dell'Agenzia. Sulla cybersicurezza come condizione per lo sviluppo di sistemi basati sull'intelligenza artificiale, quantomai efficace il testo del Considerando 76 del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale): la «cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole

andranno ulteriori compiti di carattere ispettivo e sanzionatorio, e all'Agenzia per l'Italia digitale – altra agenzia governativa che opera nel settore della digitalizzazione – spetterebbe il controllo sullo sviluppo dell'IA negli enti pubblici e la definizione delle misure di certificazione e accreditamento degli sviluppatori[38].

3. Per concludere, con alcuni interrogativi

La scelta di un modello di governo della cybersicureza tendenzialmente accentrato è confermato nei documenti di indirizzo che delineano la strategia nazionale in materia[39], per quanto le misure in essi previste cerchino di enfatizzare anche le azioni di coordinamento degli interventi di tutti i soggetti pubblici e privati coinvolti. In definitiva, siamo di fronte a questioni inedite – almeno nei termini che la cybersicurezza sta assumendo da ultimo – che impattano sul difficile equilibrio tra esigenze di sicurezza pubblica e di protezione delle libertà fondamentali, ma aprono al contempo a nuovi interrogativi[40].

Le tecniche di sicurezza informatica evolvono, per rispondere alla specializzazione e all'aumento per numero e superficie di attacco delle aggressioni, e i requisiti di sicurezza delle reti e dei sistemi di informazione si irrobustiscono in una dinamica di azione e reazione tra tecniche di hacking e di anti-hacking[41]. In questo scenario, il ruolo delle autorità pubbliche è decisivo, a patto che esse non rinuncino a valorizzare le azioni coordinate e

che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza.».

38. Dal 1993 ad oggi la "materia della digitalizzazione" è stata affidata sempre ad agenzie governative, pur con rilevanti differenze sotto il profilo organizzativo e funzionale. Dal 1993, quando fu costituita la prima Autorità per l'informatica nella pubblica amministrazione (AIPA), passando per il Centro tecnico per la Rupa (1997), il Cnipa (2003), l'Agenzia per la diffusione delle tecnologie per l'innovazione (2006), il DigitPA (2009) fino all'Agenzia Italia digitale (2012) e all'ACN.
39. La *Strategia nazionale di Cybersicurezza 2022-2026* (adottata nel maggio 2022) e il relativo Piano di implementazione, previsto dall'art. 2 co. 1, lett. b) del d.l. n. 82/2021, convertito nella legge n.109/2021 (istitutivo della Agenzia per la Cybersicurezza Nazionale - ACN), dispongono il raggiungimento di 82 nuove misure entro il 2026. Molteplici gli obiettivi: proteggere asset strategici nazionali attraverso un approccio risk based, adottando un "quadro normativo efficiente per una transizione digitale resiliente del Paese"; rispondere alle minacce e crisi cyber nazionali attraverso sistemi di monitoraggio, rilevamento, analisi e processi di sicurezza; sviluppare tecnologie digitali sicure attraverso strumenti e iniziative che supportino attività di ricerca, centri di eccellenza e imprese del settore.
40. Si pensi per esempio alla cosiddetta "direttiva Monti" (d.P.C.M. 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*) che imponeva a carico di alcuni operatori privati (es. i fornitori di servizi di comunicazione elettronica e reti pubbliche di comunicazione; i gestori di infrastrutture critiche di rilievo nazionale ed europeo) nuovi obblighi informativi a favore del Nucleo per la sicurezza cibernetica. Questi soggetti dovevano comunicare le violazioni "significative" della sicurezza o dell'integrità dei propri sistemi informatici, fornendo informazioni e dati (e quindi consentendo l'accesso a basi di dati nelle quali sono raccolti e trattati dati personali). E già al tempo le "esigenze di adempimento delle funzioni istituzionali" (di cybersicurezza) che le norme in materia di segreto e sicurezza nazionale pongono alla base di questo accesso a dati personali e sensibili in possesso di soggetti privati non parevano garanzia sufficiente per la tutela dei diritti fondamentali coinvolti. Sul punto v. ampiamente Resta 2024.
41. Il rischio inteso come potenziale perdita o perturbazione causata da un incidente deve essere valutato sulla base dell'entità della perdita o perturbazione e della probabilità che l'incidente si verifichi; questo rischio diventa poi "significativo" se ha delle caratteristiche tecniche per cui si può presumere una "probabilità elevata" di provocare un incidente con un impatto negativo grave. Così le definizioni di "rischio di cibersicurezza" (art. 1, co. 1, n. 37) e "rischio di cibersicurezza significativo" (art. 1, co. 1, n. 38) nel regolamento (UE) 2024/2847 (regolamento sulla ciberresilienza).

collettive, pilastro della sicurezza digitale, e non si limitino "solo" a normarla[42].

Si tratta in definitiva di aggiungere un tassello alla riflessione sulle "vulnerabilità" dell'attuale governance del digitale, a partire dall'osservazione delle dinamiche di governo di un settore solo all'apparenza fortemente tecnico; e di considerare nuove domande, interrogandosi anzitutto su quale sia oggi *effettivamente* la pluralità di interessi che l'esercizio della funzione pubblica di cybersicurezza mira a tutelare.

Riferimenti bibliografici

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

V. Antonelli (2017), *La sicurezza in città ovvero l'iperbole della sicurezza urbana*, in "Istituzioni del federalismo", 2017, n. 1

R. Baldoni (2024), *Charting Digital Sovereignty: A Survival Playbook. How to assess and to improve the level of digital sovereignty of a country*, independently published, 2024

F. Bavetta (2022), *Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo*, in "MediaLaws", 2022, n. 3

P. Benanti (2022), *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, 2022

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

A. Bradford (2023), *Digital Empires. The Global Battle to Regulate Technology*, Oxford University Press, 2023

M. Buffa (2023), *La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in "Democrazia e Diritti Sociali", 2023, n. 1

A. Cardone (2021), *"Decisione algoritmica" vs decisione politica? A.I., Legge, Democrazia*, Editoriale Scientifica, 2021

G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di) (2022), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, il Mulino, 2022

Clusit (2024), *Rapporto 2024 sulla sicurezza ICT in Italia*, ottobre 2024

F. Casarosa, G. Comandè (2024), *Aspettando la NIS2: ovvero il diritto privato della* cybersecurity, in "Il Diritto dell'informazione e dell'informatica", 2024, n. 1

A. Contaldo (2023), *L'attuazione della "cybersecurity" nazionale: un difficile esercizio di una funzione pubblica*, in "Lo Stato", 2023, n. 21

G. Famiglietti (2020), *Il patrocinio legale a spese della Regione nel quadro del "magnetismo securitario" (a partire da Corte cost. n. 285 del 2019)*, in "Forum di Quaderni Costituzionali", 2020, n. 2

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

42. Sulla rilevanza delle azioni collettive nel settore della cybersicurezza insiste particolarmente il National Cyber Security Center inglese (cfr. *NCSC Annual Review* cit.). Sui carichi regolatori, da ultimo v. European Commission, *The future of European competitiveness*, September 2024 (cosiddetto "Rapporti Draghi"), secondo cui sono oltre 350 gli atti normativi dell'Unione che regolano l'utilizzo delle tecnologie digitali. Tali atti gravano con oneri e obblighi specie sulle start-up che operano nei settori più innovativi. Uno stock normativo reso ancor più pesante dalla sistematica violazione da parte degli Stati membri del divieto di gold plating (cioè di superare in fase di recepimento o attuazione le misure standard contenute negli atti dell'Unione).

G. Finocchiario, L. Balestra, M. Timoteo (a cura di) (2022), *Major Legal Trends in the Digital Economy. The Approach of the EU, the US, and China*, il Mulino, 2022

G. Fiorinelli, M. Giannelli (a cura di) (2024), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, sezione monografica, in "Rivista italiana di informatica e diritto", 2024, n. 1

I. Forgione (2022), *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in "Diritto amministrativo", 2022, n. 4

M. Giannelli (2024), *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, in "Rivista italiana di informatica e diritto", 2024, n. 1

L. Golisano (2022), *Il governo del digitale: strutture di governo e innovazione digitale*, in "Giornale di diritto amministrativo", 2022, n. 6

T.F. Giupponi (2024), *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2024, n. 2

ITU (2024), *Global Cybersecurity Index 2024*, 5th edition, 2024

R. Lakshmanan (2024), *Russian RomCom Attacks Target Ukrainian Government with New SingleCamper RAT Variant*, in "The Hacker News", October 17, 2024

E. Longo (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna parlamentare", 2024, n. 2

E. Longo (2024-a), *La disciplina della cybersecurity nell'Unione europea e in Italia*, in S. Calzolaio, A. Iannuzzi, E. Longo et al., "La regolazione europea della società digitale", Giappichelli, 2024

C. Mosca (2021), *La sicurezza: valori, modelli e prassi istituzionali*, Editoriale Scientifica, 2021

G.G. Nobili (2018), *Le linee generali delle politiche pubbliche per la promozione della sicurezza integrata e la sicurezza urbana nel coordinamento tra Stato e Regioni*, in G.G. Nobili, T.F. Giupponi, E. Ricifari, N. Gallo (a cura di), "La sicurezza delle città. La sicurezza urbana e integrata", Franco Angeli, 2018

M. Pietrangelo (2024), *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in "Rivista italiana di informatica e diritto", 2024, n. 1

S. Poletti (2023), *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in "MediaLaws", 2023, n. 2

O. Pollicino (2023), *Potere digitale,* in "Potere e Costituzione", Enciclopedia del diritto, I Tematici, vol. 5, Giuffrè, 2023

F. Resta (2024), *Cybersicurezza e protezione dati: un rapporto ambivalente*, in "Rivista italiana di informatica e diritto", 2024, n. 2

G. Resta (2023), *Poteri privati e regolazione*, in "Potere e Costituzione", Enciclopedia del diritto, I Tematici, vol. 5, Giuffrè, 2023

F.N. Ricotta (2023), *Agenzia per la "cybersicurezza" nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in "Diritto penale contemporaneo", 2023, n. 1

M.A. Rizzi, F. Serini (2024), *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in "Rivista italiana di informatica e diritto", 2024, n. 2

A. Simoncini (2022), *La dimensione costituzionale dell'intelligenza artificiale*, in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), "AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale", il Mulino, 2022

A. Sola (2022), *Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*, in "MediaLaws", 2022, n. 3

F. Soro (2019), *Regolazione e governance del mondo digitale. Profili del diritto della rete in USA, UE e Italia*, Giappichelli, 2019

S. Staiano (2024), *Nel margine del caos. Trasformazione e conservazione dell'ordinamento costituzionale*, in "Rivista AIC", 2024, n. 11

L. Torchia (2024), *Poteri pubblici e poteri privati nel mondo digitale*, in "il Mulino", 2024, n. 1

R. Ursi (a cura di) (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023

R. Ursi (2022), *La sicurezza pubblica*, il Mulino, 2022

A. Vedder (2019), *Safety, Security and Ethics*, in A. Vedder, J. Schroers, C. Ducuing, P. Valcke (eds.), "Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security", Intersentia, 2019

G. Zaccaria (2022), *Postdiritto. Nuove fonti, nuove categorie*, il Mulino, 2022

F. Zorzi Giustiniani (2022), *La nuova direttiva europea per la cybersicurezza e un ulteriore ampliamento del diritto all'oblio digitale*, in "Nomos", 2022, n. 3